



FORMATION EXPERTISE : SÉCURISATION DE LA VOIP, DANGERS & SOLUTIONS

OBJECTIFS

Ce cours apporte au stagiaire, les bases théoriques et pratiques de maîtrise de la politique de sécurité dans un contexte VoIP / ToIP ou mixte voix et data. À l'issue de la formation, les stagiaires seront capables de :

- appréhender les menaces et les attaques internes et externes du monde IP, les vulnérabilités
- décrire les enjeux de la sécurité ToIP & maîtrise de la QoS,
- décrire les enjeux du codage de la voix, les solutions de cryptage
- déterminer les points clefs d'une politique de sécurité,
- comprendre les spécificités des architectures sécurisées, et les impératifs de QoS,
- différencier les différents Firewalls et leurs techniques
- déployer et administrer des firewalls.
- décrire les différentes vulnérabilités des solutions VoIP / ToIP et les solutions à mettre en place : VLAN, NAT, FireWall SIP, SBC, ...

MÉTHODE

Les exposés théoriques sont illustrés d'exemples concrets, de représentations schématiques et d'exercices pratiques. Tout au long de la formation, du temps sera consacré aux exercices et aux questions permettra d'intégrer les notions de base et de les manipuler en groupe. L'atteinte des objectifs est contrôlée au fur et à mesure du stage.

PERSONNES CONCERNÉES, PRÉREQUIS

Directeurs, responsables du système d'information, ingénieurs, techniciens, administrateurs systèmes et réseaux ayant des connaissances informatiques, TCP/IP et VoIP et devant intervenir dans le déploiement de solutions VoIP/ToIP.

DURÉE

Trois journées de formation en intra-entreprise pour 3 à 10 participants.

Introduction aux concepts de sécurité: les points clefs

- la sécurité dans les réseaux IP : Authentification, confidentialité, piratage, vol d'info, vol de trafic, spécificités des solutions VoIP / ToIP

Rappels sur TCP/IP et les services Internet

Fonctions et limites d'un firewall Data pour les applications voix

- concepts et définitions, protections d'un réseau par un firewall VoIP
- le filtrage et ses limites, NAT, PAT
- principes de reconnaissance des signatures, spécificité SIP, MGCP, H323, actions sur les flux de signalisation, sur les flux RTP

Firewall VoIP, performances des réseaux et QoS VoIP

- répartition de charges, la haute disponibilité
- Routeurs filtrants, firewalls à états, Proxies et firewalls VoIP

Sécurisation des flux Voix

- aboutement des flux RTP, Cryptage des flux RTP

Les dangers et leurs parades

- les attaques DOS, backdoor Modem et VMS, War-dialing, Invite, Cancel, Bye, Move permanently, Overflood RTP, Spam, Phreaking, ...

Les fonctionnalités des firewalls VoIP

- spécificité VoIP des solutions NAT
- fonctions avancées de FireWall (blocage les attaques DOS, Black listage, sécurisation des ports télémaintenance, protection de la configuration...)
- exemples de mise en œuvre de la sécurité, architectures sécurités
- le traitement des logs, supervision et sécurité d'un firewall

Architecture de sécurité

- les zones démilitarisées, interco d'IPBX, VPN, IP Centrex, opérateur, rôle des SBC (Session Border Controller), protection des MGC, architectures, déploiement. Exemples de mise en œuvre

Les offres du marché, exemples, conseils et sources d'information

Travaux pratiques

- Parades aux écoutes de communications et codes DTMF
- Parades aux Flooding (réseaux et applicatif)
- Parades aux usurpations d'identification/authentification