



FORMATION EXPERTISE : SÉCURITÉ DES RÉSEAUX IP partie 1/2

OBJECTIFS

Ce cours apporte au stagiaire les bases théoriques et pratiques de maîtrise de la politique de sécurité dans un contexte réseau IP et VoIP. À l'issue de la formation, les stagiaires seront capables de :

- déterminer les points clés d'une politique de sécurité,
- appréhender les menaces et les attaques internes et externes du monde des réseaux IP, les points clés d'une politique de sécurité réseau
- comprendre les bons choix pour une architecture sécurisée, tout en conservant un bon niveau de performance
- décrire les principales vulnérabilités réseaux, décrire les principes et équipements de détections et de préventions
- différencier les différents Firewalls et leurs techniques
- déployer et administrer des firewalls.
- comprendre les spécificités des architectures sécurisées, et les impératifs de QoS,
- particulièrement dans des contextes ToIP
- décrire les enjeux du codage de la voix, les solutions de cryptage
- 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 de sécurisation CoIP.

DURÉE

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

Rappels et principes

- l'évolution du SI système d'information
- les réseaux multiservices, voix, données, vidéo, la convergence
- les risques Internes et Externes
- comment supprimer 95% des attaques ? Ou trouver les informations nécessaires à la veille technologique, les sites majeurs de la sécurité

Vulnérabilités des réseaux TCP/IP

Les niveaux de vulnérabilité

- couche physique : Ethernet, point-à-point, Wi-Fi, etc.
- couche réseau : IP, couche transport : TCP/UDP
- couche services : HTTP, DNS, FTP, SMTP, etc.

Les attaques (outils et méthodes d'intrusion TCP-IP)

- attaques passives et actives
- les attaques par le noyau (IP Spoofing, TCP-flooding, SMURF, Man In The Middle, etc.).
- les attaques par les services : DNS, HTTP, SMTP, etc.
- le code vandale dans le système d'information : les virus, ver, bombe logique, trojan, etc.
- sniffing, tapping, smurfing, hi-jacking, flooding, cracking

Protections réseaux TCP/IP

Technologie firewall/proxy

- Externes/Interne, filtrage et firewall

Les catégories de Firewalls

- les routeurs filtrants, les ACL.
- le relais (proxy) et le reverse proxy,
- adressage privé (RFC 1918) et le masquage d'adresse : NAT PAT
- le filtrage : filtrer une application, les relais de filtrage dédiés/non dédiés.
- principes des firewalls, fonctions de filtrage fin.
- l'évolution du concept de DMZ (zones démilitarisées).
- les firewalls de type "Appliance", l'approche SOHO
- La redondance de firewalls : haute disponibilité, partage de charge et équilibre de charge.
- choisir un firewall : fonction et limites, critères de sélection.
- vers la détection et prévention d'intrusion réseau : NIDS et NIPS



FORMATION EXPERTISE : SÉCURITÉ DES RÉSEAUX IP PARTIE 2/2

Sécurité des échanges, bases de la cryptographie

- techniques cryptographiques
- historique, terminologie, législation, algorithmes, cryptanalyse

Chiffrement symétrique et asymétrique

- algorithmes à clé secrète : DES, IDEA, AES
- algorithmes à clé publique : schémas sans partage de secret de Diffie & Hellman, tiers de confiance, RSA, etc.

Contrôle d'intégrité, authentification, signature numérique

- intégrité : empreinte, scellement : MD5, SHA-1
- scellement et signature électronique
- mots de passe, TOKEN, carte à puce, certificats ou biométrie ?
- authentification forte : logiciels (S/KEY), cartes à puces,
- préserver la confidentialité des mots de passe.
- application de la cryptographie : schéma de confidentialité et d'intégrité, législation, produits de chiffrement
- protocoles IPSEC, SSL, SOCKS, S-HTTP, S/MIME, PGP
- évaluation des systèmes d'authentification : Radius, TACAS+, KERBEROS, etc.

Architecture de sécurité

- authentification par intégrité et confidentialité des données.
- gestion de la confiance : centre distributeur de clés ISO 8732, distribution par annuaire UIT-T X509.
- les architectures à clés publiques (Public Key Infrastructure).
- le standard SSL : SSL V2, SSL V3, TLS, 40 ou 128 bits.
- serveur de certificat privé ou public.
- certifications serveurs et clients.
- gestion des certificats : de la création à la révocation.
- la gestion des identités et l'annuaire LDAP.
- architectures "3A" (authentification, autorisation, audit), SSO,
- Kerberos et les normes OSF/DCE et ECMA TACACS.

Architecture de sécurité: VPN sur Internet

- les VPN (Virtual Private Network) Point à Point ou site to site et les VPM mobiles
- Internet et la sécurité de la messagerie d'entreprise : SPAMS,
- le standard IPSec, les protocoles AH et ESP, la gestion des clés.
- les produits compatibles IPSec, l'interopérabilité entre produits
- l'apport du protocole Radius, la gestion des profils

Spécificité de la sécurité de la Voix sur IP (VoIP)

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
- 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 RTP

Les dangers

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

Les fonctionnalités des firewalls VoIP

- spécificités 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
- interconnexion d'IPBX, VPN, IP Centrex, opérateur, rôle des Session Border Controller, protection des MGC, architectures, déploiement
- exemples de mise en œuvre

Travaux pratiques et exemples concrets d'architecture sécurisée

- VoIP/ToIP
- application web type e business
- messagerie
- VPN d'accès