Sécurité des réseaux IP

Ce cours apporte les bases théoriques et la pratique permettant la maîtrise de la politique de sécurité d'un réseau IP.

Domaine(s) : **Production des services**
Niveau(x) : **Expertise**
Durée : **4 jours**
Public(s) : **Ingénieurs et techniciens**

NOS TARIFS

Inter entreprises :
590 € H.T. par jour et par personne
Intra entreprise en présentiel :
2 100 € H.T. par jour de formation, groupe de 8 personnes maximum
Intra entreprise à distance :
2 100 € H.T. par jour de formation, groupe de 6 personnes maximum
Cours particulier :
950 € H.T. (1 personne) par jour, dans nos locaux en région parisienne ou à distance
Frais de déplacement du formateur en supplément pour toute action de formation réalisée hors région parisienne (Paris et petite couronne).

Objectifs

A l'issue de la formation, les stagiaires seront capable de :

- déterminer les points clefs d'une politique de sécurité,
- appréhender les menaces et les attaques internes et externes du monde des réseaux IP, les points clefs d'une politique de sécurité réseau
- comprendre les bons choix pour une architecture sécurisée
- décrire les principales vulnérabilités réseaux, maitriser les principes et équipements de détections et de préventionsIDS/IPS UTM Firewalls de nouvelle génération
- différencier les différents Firewalls et leurs techniques
- déployer et administrer des firewalls.
- comprendre les spécificités des architectures sécurisées

Programme

RAPPELS ET PRINCIPES

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

PROTECTIONS RÉSEAUX TCP/IP

TECHNOLOGIE FIREWALL/PROXY

- Externes/Interne, filtrage et firewall

COGICOM - Vos formations télécoms
5, rue des Vignoles - 75020 PARIS — www.cogicom.com
Contact : info@cogicom.com, +33 1 60 07 62 05

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

SÉCURITÉ DES ÉCHANGES, BASES DE LA CRYPTOGRAPHIE

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

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.
- serveurs et clients (CRL les magazins)
- 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) site to site et les VPM mobiles
- 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

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

COGICOM - Vos formations télécoms
5, rue des Vignoles - 75020 PARIS — www.cogicom.com
Contact : info@cogicom.com, +33 1 60 07 62 05

Méthodes, modalités d'évaluation

Les exposés théoriques sont illustrés d'exemples concrets et de représentations schématiques. L'atteinte des objectifs est contrôlée au fur et à mesure du stage, tout au long de la formation, par des jeux de questions-réponses et des discussions, permettant d'intégrer les notions de base et de les manipuler en groupe.

Une évaluation plus formelle est faite chaque matin à la reprise du cours, afin de valider la bonne progression du groupe et de chacun des stagiaires, par un jeu de questions-réponses.

Une évaluation par quizz ludique est organisée pendant et à la fin de la formation.

Le support de cours (env. 300 pages), impression couleur, reproduisant les slides projetées, est complété de textes, articles, témoignages.

Personnes concernées, prérequis

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

COGICOM - Vos formations télécoms
5, rue des Vignoles - 75020 PARIS — www.cogicom.com
Contact : info@cogicom.com, +33 1 60 07 62 05