Sécuriser ses réseaux IP

2 Jours **14 Heures**

Objectifs

Reconsidérer la sécurité en concevant un ensemble cohérent Identifier les actifs à protéger, leurs valeurs et les risques encourus en cas de destruction de ces actifs

Élaborer une politique de sécurité, partagée par tous les membres de l'entreprise et pour parties par ses partenaires, parfois même fournisseurs et clients

Acquérir une compréhension des fondamentaux techniques, des outils disponibles, des méthodes et contres mesures disponibles afin de concrétiser cette politique dans une mise en œuvre technique efficace

Public visé / Pré-requis

Les administrateurs réseaux, les chefs de projets

Une connaissance minimale du fonctionnement des réseaux TCP/IP. Un rappel détaillé sera effectué sur les points importants pour suivre la formation

Profil Formateur

Consultant spécialiste de la sécurité informatique

Moyens

Exposés théoriques, études de cas, démonstrations

Programme

Les réseaux, historique et rappels
Les protocoles
Ethernet
IP – ARP – ICMP – UDP – TCP – DNS

Typologie non exhaustive des menaces
Intrusion.
Déni de service
Code mobile
Ingénierie sociale
Les outils et méthodes de l'attaquant

Éléments de cryptologie
Cryptographie : présentation, historique et définitions
Les deux familles d'algorithmes, clés, signature
Confidentialité, intégrité, authentification, non répudiation

Organiser la sécurité
Méthodologie (Évaluation des risques)

Mise en œuvre technique
Pare feu (firewall), type de filtrage
Concentrateur et commutateur
Contrôle d'accès au réseau
Mandataire (proxy, reverse proxy)
Cloisonnement (dmz)
Technologies VPN
Configurer les serveurs
Défense périmétrique
Défense en profondeur
Certificats
Authentification

Détecter et réagir
IDS et IPS
Déployer un IDS
Exploitation

Les tests d'intrusion
Objectifs
Utilité

Le contexte législatif
Sécurité et Open source

Contacts : Audrey Bauduin
Control^C - 1 Place de l'Ermitage - 77000 Melun -Tél. : 01 64 39 77 99 -Fax : 01 64 10 02 84 - Site : www.controlc.fr