Sécurité Réseaux – Technologie (NSA)

Cible

Cette formation a été conçue pour fournir une connaissance théorique et pratique pour les ingénieurs de production, de maintenance ou d'études mettant en œuvre des protocoles de sécurité réseau.

Pré-requis

Les stagiaires doivent avoir suivi les formations Réseaux Industriels (CT1 et CT2) avant celle-ci ou avoir de bonnes connaissances de bases sur Ethernet ou avoir des connaissances solides sur TCP/IP. Cette formation est un prérequis conseillé pour les formations EAGLE (SP1 ou SP3)

Objectifs

Dans ce cours, les participants apprendront les bases théoriques et tous les fondamentaux liés à la sécurité réseaux : Les types de menaces et d'attaques ainsi que les moyens de protections (Firewall, crytage, ...). Une orientation sera donnée sur les besoins et les applications du monde industriel.

La sécurité des réseaux devient un critère de plus en plus important dans le monde industriel. Aujourd'hui les demandes d'interconnexion des réseaux industriels avec les réseaux d'entreprise sont de plus en plus nombreuses. Comment bénéficier de la souplesse de communication des réseaux bureautique et publics?

Il est tout à fait possible de concilier les deux, en utilisant des techniques de filtrage et sécurisations adaptées qui vous permettra de garder une totale maîtrise des accès à votre réseau industriel.

Seminar Content

Les bases de la sécurité

- Définitions
- Formes de sécurité

Les types d'attaques

- Types d'attaques
- Peurs et réalités

Service de sécurité

- Confidentialité
- Intégrité
- Disponibilité
- Responsabilité

Politique de sécurité

- Gestions des risques
- Evaluation menaces / vulnérabilités
- Processus de sécurité

Les attaquants

- Piratage
- Hackers / Crackers

Analyses des attaques

- Ingénierie sociale
- Virus, vers, chevaux de troie
- Attaques Internet
- Attaques systèmes
- Attaques de mots de passe
- Attaques d'usurpation
- Ecoutes / Interceptions
- Attaques par sondage
- Attaques de saturation

Protections

- Appareils réseau
- Routage
- VLAN

Pare-feu

- Types de Firewall / Architectures
- Mécanismes de filtrage
- Inspections de paquets
- NAT / DMZ / Proxy

Le chiffrement

- Clé symétrique
- DES, 3DES, AES
- Clé asymétrique (publique / privée)
- RSA, Diffie-Hellman
- Fonction de hachage
- Signature électronique
- MD5, SHA
- Certificats / PKI

Systèmes cryptographiques

- SSL / TLS - SSH
- S-HTTP / S-MIME
- SET / PGP / PEM

VPN

- Architectures / Tunneling
- Types de VPN
- PPP, PPTP, L2TP
- IPsec (AH ou ESP)
- SA, IKEv1 et v2

Systèmes d'Authentification

- Protocoles PAP, CHAP, MS-CHAP
- 802.1x et EAP
- Types EAP (MD5, TLS)
- Serveur Radius
- 802.11i

Détection d'Intrusion (IDS)

- Types d'IDS
- Architectures IDS

Sécurité et industrie

- Comparaison industrie/ informatique
- Besoins industriels
- Architecture à compartiments

Exercices Firewall et VPN avec EAGLE

Langues

- NSAf - Français

Durée

NSAf - 3 jours
9:00–16:30

Calendrier / lieu / prix

www.hicomcenter.com