Autour de la sécurité

Mettre en œuvre la sécurité système et réseau

SEC

SE001
5 jours

Objectifs

Grâce à ce stage, vous acquerrez la connaissance complète des différents endroits où implémenter les différentes briques de sécurité. Des laboratoires sont proposés pour mettre ne œuvre les principaux concepts.

A qui s'adresse ce cours ?

Ce cours s'adresse à toute personne ayant en charge la sécurité d'un système d'information ou intervenant sur le réseau ou la mise en lace de serveurs d'entreprise.

Pré-requis

Utilisation courante de Windows et des équipements constitutifs d'un réseau, connaissances couvertes par le cours A003-RES1 et A002 TCP-IP.

Contenu du stage

1. L'environnement
- 1.1. Le périmètre (réseau, systèmes d'exploitation, applications)
- 1.2. Les acteurs (Hackers, Responsable sécurité, auditeur, vendeurs et éditeurs, sites de sécurité)
- 1.3. Les risques
- 1.4. La protection
- 1.5. La prévention
- 1.6. La détection

2. Les attaques
- 2.1. Les intrusions de niveau 2
- 2.2. Au niveau du commutateur d'accès
- 2.3. Au niveau du point d'accès sans-fil
- 2.4. Les intrusions de niveau 3 (IP)
  - 2.4.1. IP spoofing
  - 2.4.2. Déni de service
  - 2.4.3. Scan
  - 2.4.4. Sniffer, man-in-the-middle
  - 2.4.5. Les applications stratégiques (DHCP, DNS, SMTP)
  - 2.4.6. Les applications à risques (HTTP)
- 2.5. Les attaques logiques
  - 2.5.1. Virus
  - 2.5.2. Ver
  - 2.5.3. Cheval de Troie
  - 2.5.4. Spyware
  - 2.5.5. Phishing
  - 2.5.6. Le craquage de mot de passe
- 2.6. Les attaques applicatives
  - 2.6.1. sur le système d'exploitation

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

2.6.2. sur les applications (buffer overflow)

3. Les protections

3.1. Au niveau des commutateurs d'accès
- 3.1.1. Port sécurisé sur mac-adresse
- 3.1.2. Utilisation du protocole 802.1x
- 3.1.3. VLAN Hopping
- 3.1.4. DHCP Snooping
- 3.1.5. IP source guard
- 3.1.6. ARP spoofing
- 3.1.7. Filtre BPDU
- 3.1.8. Root guard

3.2. Au niveau sans-fil
- 3.2.1. Mise en place d'une clé WEP
- 3.2.2. Mise en place de WPA
- 3.2.3. Mise en place de WPA2 (802.1i)

3.3. Au niveau IP
- 3.3.1. Les pare-feu applicatifs
- 3.3.2. Les pare-feu spécialisé
- 3.3.3. Les pare-feu sur routeur
- 3.3.4. Les pare-feu state full (inspection des couches au dessus de 3)
- 3.3.5. Les UTM
- 3.3.6. Les proxys

3.4. Protection des attaques logiques
- 3.4.1. Les anti-virus
- 3.4.2. Les anti spyware
- 3.4.3. Le concept NAC

3.5. Protection des attaques applicatives
- 3.5.1. Hardening des plate-formes Microsoft
- 3.5.2. Hardening des plate-formes UNIX
- 3.5.3. Validations des applicatifs

4. La sécurisation des accès distants

4.1. Etablissement d'un VPN

4.2. Choix cryptographique

4.3. VPN IPsec
- 4.3.1. Serveur ou boitier spécialisé ou UTM ?
- 4.3.2. Client logiciel ou matériel ?

4.4. VPN SSL
- 4.4.1. Serveur
- 4.4.2. Appliance spécialisée ou UTM ?

4.5. Principe du NAC

5. Monitoring et prévention

5.1. Sondes IDS

5.2. SysLog Serveur

5.3. Exploitations des logs

5.4. IPS
- 5.4.1. Boitiers dédiés
- 5.4.2. Fonctionnalité du routeur

6. Exemples d'architectures

6.1. Exemple d'une entreprise mono-site

6.2. Connexion des nomades

6.3. Exemple d'entreprise multi-site

7. Cadre législatif

7.1. Rappel sur le cadre légal

7.2. Rappel l'application de la LSF

Laboratoires pratiques

Lab1 : Exemple d'attaque de niveau 2 et 3
Lab 2 : Exemple de protection de niveau 2 et 3
Lab 3 : Etablissement de VPN SSL et IPsec
Lab 4 : Mise en place d'un IPS sur routeur

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00