Les bases de la sécurité systèmes et réseaux

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Connaître les failles et les menaces des systèmes d'information
- Maîtriser le rôle des divers équipements de sécurité
- Mettre en œuvre les principaux moyens de sécurisation des réseaux

Public concerné

Techniciens et administrateurs systèmes et réseaux.

Prérequis

Bonnes connaissances en réseaux et sécurité. Connaître le guide d'hygiène sécurité de l'ANSSI. Avoir suivi le parcours introductif à la cybersécurité.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Durée de la Formation :3 Jours (21 heures)

Prix de la Formation :2350 euros TTC

Les bases de la sécurité systèmes et réseaux

Programme de la formation

1 Le métier d'intégrateur sécurité

- Quel est le métier de l'intégrateur sécurité ?
- Quelles sont ses compétences ?
- Participer au maintien en conditions optimales de sécurité des OS.
- Intégrer, déployer et maintenir des solutions de sécurité.
- Les solutions de sécurité essentielles.

2 Risques et menaces

- Introduction à la sécurité.
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP SYN Flood, SMURF, etc.
- Déni de service et déni de service distribué.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- Les attaques sur le DNS.

Travaux pratiques

Installation et utilisation de l'analyseur réseau Wireshark. Mise en œuvre d'une attaque applicative.

3 Architectures de sécurité

- Quelles architectures pour quels besoins ?
- Sécurisation de l'architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité.
- Evolution technologique des firewalls (Appliance, VPN, IPS, UTM...).
- Les firewalls et les environnements virtuels.
- Reverse proxy, filtrage de contenu, cache et authentification.

Travaux pratiques

Mise en œuvre d'un proxy Cache/Authentification.

4 Sécurité des données

- Cryptographie.
- Chiffrements symétrique et asymétrique. Fonctions de hachage.
- Services cryptographiques.
- Authentification de l'utilisateur.
- Certificats X509. Signature électronique. Radius. LDAP.

- Vers, virus, trojans, malwares et keyloggers.

Travaux pratiques

Déploiement d'un proxy HTTP/FTP Antivirus. Mise en œuvre d'un certificat serveur.

5 Sécurité des échanges

- Sécurité WiFi.
- Les limites du WEP. Le protocole WPA et WPA2.
- Attaque Man in the Middle avec le rogue AP.
- Le protocole IPSec.
- Modes tunnel et transport. ESP et AH.
- Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).
- Les protocoles SSL/TLS.
- Le protocole SSH. Présentation et fonctionnalités.

Travaux pratiques

Réalisation d'une attaque Man in the Middle sur une session SSL. Mise en œuvre d'IPSec mode transport/PSK.

6 Sécuriser un système, le "Hardening"

- Critères d'évaluation (TCSEC, ITSEC et critères communs).
- Sécurisation de Windows.
- Gestion des comptes et des autorisations.
- Contrôle des services.
- Configuration réseau et audit.
- Sécurisation de Linux.

Travaux pratiques

Exemple de sécurisation d'un système Windows et Linux.