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
- Concevoir et réaliser une architecture de sécurité adaptée
- Mettre en œuvre les principaux moyens de sécurisation des réseaux
- Sécuriser un système Windows et Linux

Public concerné

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

Prérequis

Bonnes connaissances en réseaux et systèmes.

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

Durée de la formation :4 jours (28heures)

Prix de la Formation :2740 euros

Méthodes et moyens pédagogiques

Travaux pratiques

La CyberRange d'Airbus CyberSecurity est utilisée pour réaliser et jouer des scénarios réalistes comprenant de véritables cyber-attaques.

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.

Sécurité systèmes et réseaux

Programme de la formation

1 Risques et menaces

- Attaques “couches basses”.
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP-SYNflood, SMURF, etc.
- Déni de service et déni de service distribué.
- Attaques applicatives.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- DNS : attaque Dan Kaminsky.

Travaux pratiques

Connexion sur la plateforme CyberRange, prise en main d’une machine Linux/Windows pour naviguer en mode commande et graphique. Utilisation de l’analyseur réseau Wireshark.

2 Les outils au quotidien

- Les outils et techniques disponibles.
- Tests d’intrusion : outils et moyens.
- Les types de scans, détection du filtrage, firewalking.
- Détection des vulnérabilités (scanners, sondes IDS, etc.).
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure.
- Monter une architecture et s’entraîner avec CyberRange (architecture, système d’exploitations, composant, etc.).
- Les scénarios disponibles sur CyberRange : cyber-attaques (réseau, system, web), trafic (dns, ftp, ping, http), etc.

Travaux pratiques

Exécution d’un scénario sur CyberRange pour effectuer des scans de vulnérabilité web (ping, scan de port, scan vulnérabilité web, dump des utilisateurs en base de données, génération de trafic).

3 Architectures de sécurité

- Quelles architectures pour quels besoins ?
- Plan d’adressage sécurisé : RFC 1918.
- Translation d’adresses (FTP comme exemple).
- Le rôle des zones démilitarisées (DMZ).
- Sécurisation de l’architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité. Actions et limites des firewalls réseaux traditionnels.

- Proxy serveur, firewall, relais applicatif.
- Reverse proxy, filtrage de contenu, cache et authentification.

Travaux pratiques

Mise en œuvre d'un proxy cache web (Squid) sur CyberRange.

4 Sécurité des données

- Les concepts fondamentaux de la cryptographie. Les principaux outils du marché, l'offre des éditeurs.
- Tendances actuelles. L'offre antivirale, complémentarité des éléments. EICAR, un "virus" à connaître.
- Chiffrements symétrique et asymétrique. Fonctions de hachage.
- Services et concepts cryptographiques.
- Principes et algorithmes cryptographiques (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Authentification de l'utilisateur. L'importance de l'authentification réciproque.
- Gestion et certification des clés publiques, révocation, renouvellement et archivage des clés.
- L'infrastructure de gestion des clés (IGC/PKI).
- Algorithme Diffie-Hellman. Attaque de l'homme du milieu (man in the middle).
- Certificats X509. Signature électronique. Radius. LDAP.
- Vers, virus, trojans, malwares et keyloggers.

Travaux pratiques

Déploiement d'un relais SMTP et d'un proxy HTTP/FTP Antivirus.

5 Sécurité des échanges

- Le protocole IPSec.
- Présentation du protocole.
- Modes tunnel et transport. ESP et AH.
- Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).
- Les protocoles SSL/TLS.
- Présentation du protocole. Détails de la négociation.
- Analyse des principales vulnérabilités.
- Attaques sslstrip et sslsnif.
- Le protocole SSH. Présentation et fonctionnalités.
- Différences avec SSL.

Travaux pratiques

Exécution d'un scénario d'analyse des vulnérabilités SSL sur CyberRange pour mettre en évidence les vulnérabilités SSL/TLS. Réalisation d'une attaque man in the middle sur une session SSL.

6 Sécuriser un système, le "hardening"

- Présentation du hardening.
- Insuffisance des installations par défaut.
- 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.
- Configuration du noyau.
- Système de fichiers.
- Gestion des services et du réseau.

Travaux pratiques

Exemple de sécurisation d'un système Windows et Linux.

7 Audit

- Supervision et administration.
- Impacts organisationnels.
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure. Quels sont les produits disponibles ?
- Traitement des informations remontées par les différents équipements de sécurité.
- Réagir efficacement en toute circonstance.
- Veille technologique. Site de référence et panorama des outils d'audit.

Travaux pratiques

Analyse de fichiers logs système de machines sur CyberRange.

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.
Découvrez-les sur notre page Comment financer sa formation