Sécurité systèmes et réseaux, niveau 2

★★★★★

PL-50 **4 Jours (28 Heures)**

Description

Ce stage avancé vous permettra de mesurer le niveau de sécurité de votre système d'information au moyen d'outils de détection d'intrusions, de détection de vulnérabilités, d'audit... Il vous apportera la connaissance de solutions avancées pour maintenir et faire évoluer dans le temps le niveau de sécurité souhaité au regard de vos besoins. Les travaux pratiques proposés permettront d'acquérir les compétences nécessaires à l'installation, la configuration et l'administration des applications les plus utilisées dans le domaine de la sécurité.

À qui s'adresse cette formation ?

Pour qui

Responsable, architecte sécurité. Techniciens et administrateurs systèmes et réseaux.

Prérequis

Aucune

Les objectifs de la formation

- Mesurer le niveau de sécurité de votre système d'information Utiliser des outils de détection d'intrusions, de détection de vulnérabilités et d'audit Renforcer la sécurité de votre système d'information Mettre en oeuvre une architecture AAA (Authentication, Autorization, Accounting) Mettre en oeuvre SSL/TLS

Programme de la formation

Rappels

- Le protocole TCP/IP.
- La translation d'adresses.
- L'architecture des réseaux.
- Le firewall : avantages et limites.
- Les proxys, reverse-proxy : la protection applicative.
- Les zones démilitarisées (DMZ).

Les outils d'attaque

- Paradigmes de la sécurité et classification des attaques.
- Principes des attaques : spoofing, flooding, injection, capture, etc.
- Librairies : Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
- Outils : Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.
- Travaux pratiques Analyse de protocoles avec Wireshark.
- Utilisation de Scapy et Arpspoof.

La cryptographie, application

- Les services de sécurité.
- Principes et algorithmes cryptographique (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Certificats et profils spécifiques pour les divers serveurs et clients (X509).
- Protocole IPSEC et réseaux privés virtuels (VPN).
- Protocoles SSL/TLS et VPN-SSL.
- Problématiques de compression des données.
- Travaux pratiques Prise en main d'openssl et mise en oeuvre d'OpenPGP.
- Génération de certificats X509 v3.

Architecture AAA (Authentication, Autorization, Accounting)

- Le réseau AAA : authentification, autorisation et traçabilité.
- One Time Password : OTP, HOTP, Google Authentificator, SSO (Protocole Kerberos).
- La place de l'annuaire LDAP dans les solutions d'authentification.
- Les module PAM et SASL.
- Architecture et protocole Radius (Authentication, Autorization, Accounting).
- Les attaques possibles.
- Comment se protéger.
- Travaux pratiques Attaque d'un serveur AAA.

Détecter les intrusions

- Les principes de fonctionnement et méthodes de détection.
- Les acteurs du marché, panorama des systèmes et applications concernés.
- Les scanners réseaux (nmap) et applicatifs (web applications).
- Les IDS (Intrusion Detection System).
- Les avantages de ces technologies, leurs limites.
- Comment les placer dans l'architecture d'entreprise.
- Panorama du marché, étude détaillé de SNORT.
- Travaux pratiques Installation, configuration et mise oeuvre de SNORT, écriture de signature d'attaques.

Vérifier l'intégrité d'un système

- Les principes de fonctionnement.
- Quels sont les produits disponibles.
- Présentation de Tripwire ou AIDE (Advanced Intrusion Detection Environment).
- L'audit de vulnérabilités.
- Principes et méthodes et organismes de gestion des vulnérabilités.
- Site de référence et panorama des outils d'audit.
- Définition d'une politique de sécurité.
- Etude et mise en oeuvre de Nessus (état, fonctionnement, évolution).
- Travaux pratiques Audit de vulnérabilités du réseau et serveurs à l'aide de Nessus et Nmap.
- Audit de vulnérabilités d'un site Web.

Gérer les événements de sécurité.

- Traitement des informations remontées par les différents équipements de sécurité.
- La consolidation et la corrélation.
- Présentation de SIM (Security Information Management).
- Gestion et protocole SNMP : forces et faiblesses de sécurité.
- Solution de sécurité de SNMP.
- Travaux pratiques Montage d'attaque SNMP.

La sécurité des réseaux Wi-Fi

- Comment sécuriser un réseau Wi-Fi ? Les faiblesses intrinsèques des réseaux Wi-Fi.
- Le SSID Broadcast, le MAC Filtering, quel apport ? Le WEP a-t-il encore un intérêt ? Le protocole WPA, première solution acceptable.
- Implémentation WPA en mode clé partagée, est-ce suffisant ? WPA, Radius et serveur AAA, l'implémentation d'entreprise.
- Les normes 802.
- 11i et WPA2, quelle solution est la plus aboutie aujourd'hui ? Travaux pratiques Configuration des outils pour la capture de trafic, scan de réseaux et analyse de trafic WIFI, injection de trafic, craquage de clés WIFI.
- Configuration d'un AP (Point d'acces) et mise oeuvre de solutions de sécurité.

La sécurité de la téléphonie sur IP

- Les concepts de la voix sur IP.
- Présentation des applications.
- L'architecture d'un système VoIP.
- Le protocole SIP, standard ouvert de voix sur IP.
- Les faiblesses du protocole SIP.
- Les problématiques du NAT.
- Les attaques sur la téléphonie sur IP.
- Quelles sont les solutions de sécurité ?

La sécurité de la messagerie

- Architecture et fonctionnement de la messagerie.
- Les protocoles et accès à la messagerie (POP, IMAP, Webmail, SMTP, etc.
-).
- Problèmes et classifications des attaques sur la messagerie (spam, fishing, usurpation de l'identité, etc.
-).
- Les acteurs de lutte contre le SPAM.
- Les méthodes, architectures et outils de lutte contre le SPAM.
- Outils de collecte des adresses de messagerie.
- Les solutions mises en oeuvre contre le SPAM.