OBJECTIFS PÉDAGOGIQUES
- Maîtriser les techniques et les outils de sécurisation, de protection et d'analyse d'intrusion afin de déployer une stratégie de sécurisation optimale

Détails::

Référence

FORLI08

Durée : 4 jours

Profil participants : Administrateurs systèmes, administrateurs réseaux, analystes de sécurité

Animateur : Consultant informaticien spécialiste en formation Linux

Pré-requis : Bonne connaissance de l'administration d'un système Linux

Dates des sessions de l'année :

- du 18 au 21 mars 2019
- du 17 au 20 juin 2019
- du 31 septembre au 03 octobre 2019
- du 02 au 05 décembre 2019

Tarif (H.T.) : 1089 €

||||Programme::

Concepts fondamentaux

Concepts de cryptologie : algorithmes, protocoles, clés privées/publiques
Les divers virus et les types d'attaques : Trojans, Worms, Spoofing…)
Comprendre les échanges réseaux IPV4 et IPV6

Techniques de sécurité locale

Sécuriser les applications d'authentification avec PAM
Sécuriser l'accès à la console d'administration avec GRUB
La sécurité de type Type Enforcement avec SELinux
Commandes d'audit de base : aide, tripwire…

Techniques de filtrage des paquets (iptables) et des pare-feu (shorewall)

Techniques de sécurité réseau

Le protocole et les commandes SSH (ssh, scp, ssh-keygen, ssh-agent…)
Présentation de la solution globale de type SSO : Kerberos
Mise en œuvre d'un système de sécurité de type PKI avec OpenCA
Sécurisation des services Internet (Web, DNS…) et de la messagerie
Mise en œuvre de VPN (IPSec, OpenVPN)

Techniques d'intrusion éthiques

Comment maîtriser les techniques des «Hackers» pour mieux se défendre
Techniques et outils pour tenter de craquer les mots de passe
Analyse des paquets TCP/IP (tcpdump, wireshark, dsniff, ettercap)
Balayage de ports (nmap) et simulation d'intrusion (nessus))
Présentation de la solution de détection d'intrusion réseau : snort

Le processus init
Le démarrage des services (init System V, Upstart, Systemd)
L'arrêt du système (shutdown)