Classe virtuelle "Linux système sécurisé" par Pythagore F.D.

La sécurité des systèmes Linux est d'autant plus importante qu'il s'agit souvent de serveurs en réseau permettant un accés aux données vitales de l'entreprise. Les mécanismes à mettre en place seront les mêmes que sur les serveurs Unix propriétaires, mais avec quelques particularités et possibilités supplémentaires (par exemple, au niveau de la sécurité du noyau sur lequel il est possible d'intervenir).Cette formation permet d'apprendre à configurer les mécanismes de sécurité des systèmes Linux.

Pythagore F.D. propose des sessions de cours en classes virtuelles. Le fonctionnement de cette solution est simple : mettre à disposition de chaque participant un espace de travail qui lui est propre et ce, depuis son environnement de travail habituel.
Ainsi, en plus de permettre d'eviter les déplacements des stagiaires ou des formateurs, l'originalité de cette solution réside dans la mise à disposition complète de l'environnement de travail nécessaire à la réalisation de l'ensemble de la formation : des supports de cours à la configuration matérielle et logicielle nécessaire à la réalisation de travaux pratiques ...
Nos équipes de développement ont travaillé à la mise en place d'un ensemble d'outils permettant de préserver la qualité pédagogique à travers l'enseignement à distance.

Pythagore F.D. organise une formation en classe virtuelle « Linux système sécurisé » du 17 au 19 Mars 2014.

Ce stage permet de savoir configurer les mécanismes de sécurité de Linux.

Le programme de la formation « Linux système sécurisé » est le suivant :

Introduction
Le besoin, définition du D.I.C.
Les attaques possibles.
Evaluation des risques.
Méthodes de protection.

Gestion utilisateurs
Rappels sur les notions de base de sécurité sur Unix :
modes d'accès, comptes utilisateurs, groupes, utilisateurs génériques de gestion de ressources.
Fichiers /etc/passwd, /etc/group, /etc/shadow.
Codage des mots de passe.
Création, modification, suppression de comptes utilisateurs.
Gestion des groupes :
ajout, retrait d'utilisateurs, création d'administrateurs de groupes.
Affectation d'un mot de passe au groupe.
Vérification de cohérence : pwck.
Connexions du compte root, contrôle de connexions.
Outil de recherche de mots de passe.
Travaux pratiques :
installation et mise en oeuvre de l'outil "John the ripper" en mode "single-crack".
Prise de privilèges : sudo, sudoers.

Authentification
pam: gestion des modules d'authentification.
Présentation et exemples d'utilisation.
Principe de base, configuration.
Les modules : différents types de modules (auth, account, session, password).
Notion de pile de modules.
Travaux pratiques :
mise en oeuvre de PAM et de quelques modules parmi les plus courants :
access, chroot, cracklib, env, ftp, groups, limits, listfile, mkhomedir, tally, time, unix, wheel

Sécurisation traitements
Les risques : le déni de service, exemples de virus sur un système Linux.
Travaux pratiques :
exploitation d'un débordement de pile.
Les moyens de détection, la surveillance, les traces :
syslog, l'accounting.

L'audit de securité.
Méthodes de protection : démarche sur les systèmes Linux.

Sécurité du noyau
Les différentes approches de sécurisation du noyau.
Présentation de GrSecurity et SELinux.
Travaux pratiques avec GrSecurity :
installation, configuration du noyau, paramétrage du niveau de sécurité.
Administration avec grAdm2.
Génération d'une politique : learning mode.
Mise en place des règles d'ACL.
L'ACL GrSec.
Restrictions d'accès aux appels systèmes. Masquage de processus.
Visibilité du répertoire /proc.
Restrictions chroot.
SELinux : principe, configuration du noyau, options du noyau.
Travaux pratiques :
définition d'une politique de sécurité.
Installation et activation de la politique de sécurité dans le fichier /etc/selinux/config.

Sécurité des données
Contrôle de la cohérence du système de fichiers : fsck.
Procédure de vérification.
Sauvegardes : définitions
Commandes et outils standards.
Utilisation des sauvegardes pour la disponibilité des données.
Outils sauvegarde/archivage/compression :
gzip, zip, tar, dump, restore, dd, cpio, rsync
Service d'urgence pour Linux :
en cas de problème au démarrage du système,
utilisation d'un système tiers : "systemRescue CD"
Travaux pratiques :
création de CD de secours.

Sécurité système de fichiers
Sécurité: mise en place des contrôles d'accès
ACL : principe des listes de contrôle d'accès POSIX.
Travaux pratiques : mise en place des ACL sur xfs
Les quotas : principe, mise en place dans le fichier /etc/fstab.
La commande edquota pour l'édition, et le paramétrage, et la commande quota pour la visualisation.
Travaux pratiques : mise en place des quotas
