Linux - Sécurisation avancée

Mise à jour : Fév. 2024

Durée : 3 jours - 21 heures

OBJECTIFS PÉDAGOGIQUES

- Connaître les failles du système, savoir s'en protéger et surveiller les accès

PRÉREQUIS

- Administrateurs système ou réseau, responsables informatiques, autres professionnels de l'informatique
- Pratique courante de Linux en tant qu'administrateur

PARTICIPANTS

- Cette formation s'adresse aux administrateurs infrastructure et système

MOYENS PÉDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Remise d'un support de cours

MODALITÉS D'ÉVALUATION

- Feuille de présence signée en demi-journée
- Evaluation des acquis tout au long de la formation
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Positionnement préalable oral ou écrit
- Evaluation formative tout au long de la formation
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

MOYENS TECHNIQUES EN PRÉSENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard

MOYENS TECHNIQUES DES CLASSES À DISTANCE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur
- Les formations en distanciel sont organisées en Inter-Entreprises comme en Intra-Entreprise
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré
- Les participants reçoivent une invitation avec un lien de connexion
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition auprès de notre équipe par téléphone au 03 25 80 08 64 ou par mail à secretariat@feep-entreprises.fr

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

ACCESSIBILITÉ

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation. Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages

Programme de formation

Linux / Unix et la sécurité

- Parvenir à la sécurité de Linux / Unix
- Détecter les intrusions avec audits/journaux
- Éviter des défauts de sécurité
- Identifier les vulnérabilités d'un logiciel et les erreurs de configuration
- Protection avec la cryptographie
- PGP (Pretty Good Privacy)
- GnuPG (Gnu Privacy Guard)
- Authenticité et intégrité grâce aux signatures numériques et aux « hash codes »

Renforcer l'authentification

- Connexion au réseau
- Risque des protocoles d'applications
- Authentification plus forte lors de la connexion grâce à la cryptographie et aux jetons
- Mise en tunnel de protocoles d'application avec SSH

Limiter les privilèges utilisateur

- Contrôle de l'accès aux racines
- Configuration de terminaux sûrs
- Empêcher l'accès aux réseaux non sécurisés
- Acquérir des privilèges root avec su
- Utilisation de groupes au lieu de l'identité root
- Contrôle de l'accès basé sur le rôle (RBAC)
- Risques de l'accès « tout ou rien » de Linux / Unix
- RBAC avec Solaris
- Ajout de RBAC avec sudo

Sécuriser les systèmes de fichiers locaux et en réseau

- Structure et partitionnement de répertoires
- Fichiers, répertoires, périphériques et liens
- Utilisation de partitions en lecture seule
- Permissions d'accès et propriété
- Fichiers immuables et en ajout seul
- Vulnérabilités de NFS
- Renforcement des systèmes Linux / Unix
- Amélioration de l'assurance de l'information avec yassp, TITAN et Bastille
- Scan de réseaux avec Nessus pour déceler les vulnérabilités
- Détection de mauvais choix de configuration avec Sussen

Éviter l'exécution de programmes

- Risques provenant d'exécutions non souhaitées de programmes
- Démarrage subreptice des programmes
- Exécution de programmes en tant qu'autre utilisateur
- Planification de programmes avec cron et at
- Diminution des vulnérabilités dans les scripts de démarrage
- Réagir aux attaques et aux intrusions
- Trouver des signes d'intrusion dans des données syslog
- Analyse d'un système compromise

Réduire les effets des exploits de BO (buffer overflow)

- Minimiser les risques des services réseau
- TCP/IP et ses points faibles de sécurité
- Sniffer des mots de passe avec Ethereal et dsniff
- Tester l'exposition du réseau avec netstat, isof et nmap
- La sécurité des services réseau internes
- Amélioration des enregistrements
- Configuration de OpenSSH et OpenSSL
- Authentification du réseau avec Kerberos
- Système X Window : vulnérabilités/solutions
- Connexion sûre aux réseaux externes
- Contrôle et enregistrement de l'accès aux serveurs avec des tcp wrappers et xinetd
- Réduction des problèmes de « buffer overflow »
- Réduction des fuites d'information
- Sécurisation des accès de type messagerie, FTP et Web (sécurisation des ports)