Linux - Sécurisation avancée

Informatique

Sécurité logicielle

Référence : 4-UX-SEC
Durée : 3 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1400 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2026 au 31/12/2026

Objectifs

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

Prérequis

Pratique courante de Linux en tant qu'administrateur

Public concerné

Administrateurs système ou réseau, responsables informatiques, autres professionnels de l'informatique.

Contenu pédagogique

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)

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants 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.
- Alternance entre apports théoriques et exercices pratiques (en moyenne sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.

- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- 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
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

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

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Nos sessions INTER 2026

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2026

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55