

LINUX - SÉCURISATION AVANCÉE

Durée	3 jours	Référence Formation	4-UX-SEC
--------------	----------------	----------------------------	-----------------

Objectifs

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

Participants

Cette formation s'adresse aux administrateurs infrastructure et système

Pré-requis

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

Pratique courante de Linux en tant qu'administrateur

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.

Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.

En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.

Formateur expert dans son domaine d'intervention

Apports théoriques et exercices pratiques du formateur

Utilisation de cas concrets issus de l'expérience professionnelle des participants

Réflexion de groupe et travail d'échanges avec les participants

Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME

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 détecter 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)



CAP ÉLAN FORMATION

www.capelanformation.fr - Tél : 04.86.01.20.50

Mail : contact@capelanformation.fr

Organisme enregistré sous le N° 76 34 0908834

version 2025