Sécurité Linux

Référence : **SECSL** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaissances en administration Linux. • Connaissances en réseau. • Connaissances en système virtualisé.

PROFIL DES STAGIAIRES

• Administrateurs. • Consultants. • Ingénieurs / Techniciens.

OBJECTIFS

• Ajouter des mécanismes de protection : Bien configurer son firewall, Compléter son firewall avec d'autres mécanismes, Isoler l'exécution des applications. • Définir une politique de sécurité efficace : Définir les besoins des clients , Identifier les points de sensibilité , Choisir une politique efficace. • Mettre en place une politique de sécurité efficace : Connaître les dangers de configuration Linux , Comprendre la sécurité mise en place , Déployer des configurations robustes.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1

Présentation des politiques de sécurité

Présentation du système Linux

Mise en place des premières sécurisations

- Secure Boot
- Grub
- Attaques DMA

Sécurisation du Noyau

- Compilation du noyau
- GRSEC
- Système auditing
- Manipulation des services
- Mise à jour
- Journalisation
- Automatisation

JOUR 2

Gestion des droits et des accès

- RWX
- Gestion des identités
- Le système d'authentification PAM
- Kernel capabilities
- SELinux
- Principe du privilège minimum

Gestion du réseau

- Filtrage des entrées réseau

Chiffrement du disque

- dm-crypt
- LUKS

Protection de la mémoire

- Bit NX
- ASLR
- Stack canary

JOUR 3

Configurer et sécuriser ses services

- SSH
- Samba
- OpenSSL
- Apache
- MySQL

Isolation des applications

- CHROOT
- Docker et durcissement