EduGroupe
Accompagner pour réussir

Sécurité Linux

Référence : **SECLINUX** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir les bases en administration de systèmes Unix, idéalement 3 à 5 ans d'expérience.

PROFIL DES STAGIAIRES

• 1-Professionnels de la sécurité. • 2-Administrateurs systèmes expérimentés. • 3-Auditeurs et gestionnaires d'incidents. • 4-Analystes en sécurité, auditeurs et membres de CSIRT (CERT).

OBJECTIFS

• Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux. • Réduire ou éliminer les risques sur les systèmes Linux. • Configurer les services courant pour qu'ils soient robustes avant mise en production (Apache, BIND, ...). • S'assurer de l'intégrité des données sur les serveurs Linux. • Maîtriser les outils permettant de répondre aux incidents de sécurité. • Améliorer ses connaissances des procédures, bonnes pratiques et outils de sécurité du monde Unix.

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

Introduction

• Panorama de l'histoire des problèmes de sécurité : Suivre l'actualité ; Implication des utilisateurs ; Discipline des administrateurs (Sudo)

Cryptographie

• Rappels sur le vocabulaire, les principes et les algorithmes
• SSH
• GnuPG
• Certificats X.509 et infrastructures à clés publiques (openssl)
• Certificats X.509 pour le chiffrement, la signature et l'authentification : application à Apache et nginx ; application à Postfix
• Systèmes de fichiers chiffrés : dm-crypt ; eCryptfs
• DNS et cryptographie : DNSSEC

Sécurité de l'hôte

• Durcissement de l'hôte : configuration de GRUB ; configuration du système ; bonnes pratiques de configuration des daemons ; Détection d'intrusion sur l'hôte ; Syslog ; comptabilité système (accounting) ; audit ; détection de rootkits ; AIDE
• Gestion des utilisateurs et authentification : NSS ; PAM

Contrôle d'accès

• Contrôle d'accès discrétionnaire : droits d'accès ; ACL
• Contrôle d'accès obligatoire : SELinux

Sécurité réseau

- Durcissement du réseau : nmap ; tcpdump ; Wireshark
- Filtrage de paquets : concepts et vocabulaire ; netfilter ; TCP Wrapper
- Réseaux privés virtuels : OpenVPN