EduGroupe
Accompagner pour réussir

Sécurité Linux

Référence : **SECLINUX** Durée : **5 jours (35 heures)** Certification : **Aucune**

Connaissances préalables

- 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 préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

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

Contenu du cours

1. Introduction

- Panorama de l'histoire des problèmes de sécurité : Suivre l'actualité

2. 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
- Systèmes de fichiers chiffrés : dm-crypt
- DNS et cryptographie : DNSSEC

3. Sécurité de l'hôte

- Durcissement de l'hôte : configuration de GRUB
- Gestion des utilisateurs et authentification : NSS

4. Contrôle d'accès

- Contrôle d'accès discrétionnaire : droits d'accès
- Contrôle d'accès obligatoire : SELinux

5. Sécurité réseau

- Durcissement du réseau : nmap
- Filtrage de paquets : concepts et vocabulaire
- Réseaux privés virtuels : OpenVPN

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.