Sécurité Réseaux Linux

Format :
Présentiel et/ou Distanciel

Durée :
3 jours / 21 h

Référence :
PRO-SEC-0162

Type de formation :
Formation qualifiante

Public :
Ce cours s'adresse aux administrateurs de serveurs et de réseaux ayant le souci de mettre en oeuvre des serveurs sécurisés.

Personnes en situation de handicap :
Vous êtes en situation de handicap et vous souhaitez faire une formation ?
Merci de bien vouloir nous contacter en amont afin d'étudier ensemble vos besoins et les solutions les plus adaptées.

Objectifs de développement des compétences :
Ce cours très pratique vous montrera comment définir une stratégie de sécurité, sécuriser des serveurs Linux au moyen d'outils et logiciels libres, et maintenir un niveau de sécurité constant dans le temps. Le cours prévoit entre autres la sécurisation du système «isolé», la sécurisation du réseau dans l'entreprise, ainsi que le nécessaire pour mener à bien un audit de sécurité.

Pré-requis :
Avoir de bonnes connaissances en administration des systèmes et réseaux.

Compétences et méthodes pédagogiques :
Les prestations de formation sont assurées par des formateurs professionnels qui utilisent des moyens pédagogiques adaptés.
Dans le cadre de session intra entreprise, possibilité de travailler sur vos projets afin de répondre à vos besoins spécifiques.
Supports de cours pédagogiques imprimés et/ou numérisés.

Répartition du temps (environ) :

Théorique 45%, Pratique 55%

Modalités d'évaluation :

Questionnaire d'auto-positionnement:
Un questionnaire d'auto-positionnement est adressé aux stagiaires en amont de la formation afin de l'adapter aux besoins et attentes des participants.

Évaluation à chaud par le biais de travaux pratiques.

- Exercices, tests d'évaluations (QUIZZ ou QCM ...).

Moyens techniques et pédagogiques :

Salle(s) de cours équipée(s) des moyens audiovisuels avec le matériel adapté à la formation (si besoin, ordinateur par stagiaire).

Modalité et délai d'accès à la formation :

Toutes nos formations sont réalisées à la demande et en fonction des souhaits de nos clients.
Nous pouvons également réaliser des formations sur-mesure à partir de programmes existants ou en construisant un programme spécifique à partir de vos objectifs.
Merci donc de bien vouloir nous contacter par courriel ou par téléphone afin de définir ensemble les dates et modalités de formation souhaitées.

Tarif :

Nous contacter pour devis personnalisés.

Programme de la formation

1. Introduction

Pourquoi sécuriser un système ?
Définir une stratégie d'authentification sécurisée.
Découvrir les différents algorithmes de chiffrement. Chiffrement d'un mot de passe. Vérification d'un mot de passe.
Voir des exemples d'attaques par dictionnaire.

2. La sécurité et l'Open source

Voir les avantages de l'open source : les corrections sont rapides, les bugs rendus publics.
Connaître la technique d'approche d'un hacker : connaîtreles failles, savoir attaquer. Exemple d'une vulnérabilité et solution de sécurisation. Quelle solution ?

3. L'installation trop complète : exemple Linux

Installer Linux : Debian, RedHat et les autres distributions.
Eviter le piège de l'installation facile. Méthodes d'ajout ou de suppression de composants logiciels.
Alléger le noyau. Drivers de périphériques, fonctionnalités, etc.

4. La sécurité locale du système

Voir des exemples de malveillance et ... d'inadvertance.
Définir une faible permissivité par défaut. Vérificationdes droitsdes fichiers, scripts et commandes efficaces pour diagnostiquer. Vérification automatisée : un changement de droit est-il légitime ?
Voir l'importance des droits sur les répertoires.
Connaître les avantages du montage d'un FS en lectureseule. Les attributs des fichiers, disponibilité et intérêt,gestion de l'effacement physique. Les outils comme Tripwire.
Conserver les logs, combien de temps, pour quoi faire ?
L'outil d'analyse des logs : logwatch.
Réagir en temps réel : exemple de script. Utiliser RPM comme HIDS.
Paramétrer PAM dans les différents contextes.
Confiner l'exécution des processus.
Découverte de la terminologie DAC, MAC, RBAC,contexte, modèle...
Définir la politique de sécurité.
Voir les outils d'administration.

5. La sécurité au niveau réseau

Utiliser un firewall
Utiliser les wrappers
Mettre en place des filtres d'accès aux services.
Configurer un firewall de manière sécurisée.
Connaître les commandes de diagnostic.
Mettre en place un firewall NetFilter sous Linux.
Découverte de la philosophie et de la syntaxe de iptables.
Voir le super-serveur xinetd. Les restrictions d'accès par le wrapper, les fichiers de trace. Réaliser un audit des services actifs.
Paramétrer ssh.

6. Les utilitaires d'audit de sécurité

Voir les produits propriétaires et les alternatives libres.

Découvrir Crack, John the Ripper, Qcrack.

Découverte des systèmes de détection d'intrusion HIDS et NIDS.

Tester la vulnérabilité avec NESSUS.

Mettre en oeuvre d'un outil de sécurité.

Nous contacter :

Dominique Odillard : 05 24 61 30 79

Version mise à jour le 24/07/2023