Formation Sécuriser un système Linux/Unix

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Ce stage très pratique vous montrera comment définir une stratégie de sécurité, sécuriser des serveurs Linux et maintenir un niveau de sécurité. 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.

Référence	SRX
Durée	3 jours (21h)
Tarif	1 950 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 10 au 12 juin 2024
du 9 au 11 septembre 2024
du 25 au 27 novembre 2024

PARIS

du 3 au 5 juin 2024
du 2 au 4 septembre 2024
du 18 au 20 novembre 2024

LYON

du 10 au 12 juin 2024
du 9 au 11 septembre 2024
du 25 au 27 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| Mesurer le niveau de sécurité de votre système Linux/Unix
| Connaître les solutions de sécurisation du système
| Mettre en place la sécurité d'une application Linux/Unix
| Établir la sécurisation au niveau réseau

Public

| Techniciens et administrateurs systèmes et réseaux.

Prérequis

| Bonnes connaissances en administration des réseaux et des systèmes.

Programme de la formation

Introduction
| Pourquoi sécuriser un système ?
| Définir une stratégie d'authentification sécurisée.
| Les différents algorithmes de chiffrement. Chiffrement d'un mot de passe. Vérification d'un mot de passe.
| Exemples d'attaques par dictionnaire.

La sécurité et l'Open Source
| Les corrections sont rapides, les bugs rendus publics.
| La technique d'approche d'un hacker : connaître les failles, savoir attaquer.
| Exemple d'une vulnérabilité et solution de sécurisation. Quelle solution ?

L'installation trop complète : exemple Linux
| Debian, RedHat et les autres distributions.
| Eviter le piège de l'installation facile.
| Allégement du noyau. Drivers de périphériques.
| Travaux pratiques : Optimisation des installations dans une optique de gestion de la sécurité.

La sécurité locale du système
| Exemples de malveillance et d'inadvertance.
| Faible permissivité par défaut. Vérification des droits des fichiers, scripts et commandes efficaces pour diagnostiquer.
| FS en lecture seule : les attributs des fichiers, disponibilité et intérêt. Outils Tripwire.
| Conservation des logs, combien de temps ?
| L'outil d'analyse des logs : logwatch. Réagir en temps réel : exemple de script. Utiliser RPM comme HIDS.
| Paramétrage de PAM dans les différents contextes.
| Confinement de l'exécution des processus. Terminologie DAC, MAC, RBAC,

contexte, modèle...
| Travaux pratiques : Travail sur les droits, les logs et les processus.

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.
| Les commandes de diagnostic. Mise en place d'un firewall NetFilter sous Linux.
| Philosophie et syntaxe de iptables.
| Le super-serveur xinetd. Les restrictions d'accès par le wrapper, les fichiers de trace.
| Réaliser un audit des services actifs. Le ssh.
| Travaux pratiques : Configurer un firewall. Auditer les services fonctionnels.

Les utilitaires d'audit de sécurité
| Les produits propriétaires et les alternatives libres.
| Crack, John the Ripper, Qcrack.
| Les systèmes de détection d'intrusion HIDS et NIDS.
| Tester la vulnérabilité avec Nessus.
| La mise en oeuvre d'un outil de sécurité.
| Travaux pratiques : Mise en oeuvre de quelques outils.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.