Sécuriser un système Linux

Les techniques de sécurisation d'un système Linux

Présentiel ou en classe à distance

4 jours (28 h)
+ certificat optionnel

Prix inter : 2.490,00 € HT
Forfait intra : 7.290,00 € HT

Réf.: XW305



La sécurité informatique est devenue une préoccupation essentielle des entreprises et organisations et donc des responsables informatiques. La sécurisation de Linux est paradoxale : d'un côté, c'est un système qui peut être extrêmement hermétique et d'un autre côté, il est souvent très vulnérable compte tenu des nombreuses possibilités de configuration offertes. Cette formation permettra aux participants de découvrir l'ensemble des techniques de sécurisation d'un système Linux.
Cette formation prépare à la certification Administrer un système Linux.

A qui s'adresse cette formation ?

- Administrateurs systèmes et réseaux expérimentés

- Avoir suivi les formations "Linux administration niveau 1 - Installation et mise en oeuvre" (XW302) et "Linux administration niveau 2 - Gestion et maintenance" (XW303) ou connaissances équivalentes
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

Pendant

1 - Les enjeux de la sécurité

- Les attaques, les techniques des hackers
- Panorama des solutions
- La politique de sécurité

2 - La cryptologie ou la science de base de la sécurité

- Les concepts de protocoles et d'algorithmes cryptographiques
- Les algorithmes symétriques et asymétriques (à clé publique), les fonctions de hachage
- La signature numérique, les certificats X-509, la notion de PKI

3 - Les utilisateurs et les droits

- Rappels sur la gestion des utilisateurs et des droits, les ACLs
- La dangerosité des droits d'endossement
- La sécurité de connexion, le paquetage SHADOW

4 - Les bibliothèques PAM

- L'architecture du système PAM, les fichiers de configuration
- L'étude des principaux modules

5 - Le système SELinux ou la sécurité dans le noyau

- L'architecture du système SELinux
- Modifier les règles de comportement des exécutables

6 - Les principaux protocoles cryptographiques en client/serveur

- SSH, le protocole et les commandes ssh
- SSL, l'utilisation de SSL et des certificats X-509 dans Apache et stunnel
- Kerberos et les applications kerbérorérisées

7 - Les pares-feux

- Panorama des techniques pares-feux
- L'architecture Netfilter/Iptables, la notion de chaine, la syntaxe d'iptables
- La bibliothèque tcpd ou l'enveloppe de sécurité, la sécurisation via xinetd
- Mise en place d'un routeur filtrant, du masquerading et d'un bastion avec iptables
- Le proxy SQUID

8 - Les VPN

- Panorama des techniques tunnels et VPN
- Le logiciel OpenVPN

9 - La sécurisation des applications

- Principes généraux
- Sécurisation du Web, d'email, du DNS, du FTP

10 - Les techniques d'audit

- L'audit des systèmes de fichiers avec AIDE et Tripwire
- Les outils d'attaque réseau
- La détection des attaques avec snort



Les objectifs de la formation

- Comprendre comment bâtir une sécurité forte autour de Linux
- Savoir mettre en place la sécurité d'une application Linux
- Comprendre les fondamentaux de la sécurité informatique et notamment de la sécurité réseau
- Être capable de sécuriser les échanges réseaux en environnement hétérogène grâce à Linux



Certificat

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Le passage en revue des différents aspects de la sécurisation de systèmes Linux.
- En accordant une large place à la pratique, ce programme favorise un ancrage durable et efficace des acquis.
- Le partage des techniques et bonnes pratiques garantissant une mise en oeuvre efficace d'une sécurité sur-mesure.
- 80% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques.
Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Dates et villes 2027 - Référence XW305

Dernières places disponibles Session garantie

A distance

du 11 janv. au 14 janv.	du 20 sept. au 23 sept.
du 18 mai au 21 mai	du 2 nov. au 5 nov.

Paris

du 11 janv. au 14 janv.	du 20 sept. au 23 sept.
du 18 mai au 21 mai	du 2 nov. au 5 nov.