



SÉCURITÉ LINUX - PERFECTIONNEMENT

3000 € HT (tarif inter) | REF : SYS733
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Ce module doit permettre aux apprenants de tester la sécurité de leurs serveurs et de mettre en évidence les risques liés aux différents éléments.

PROGRAMME

Introduction à la sécurité

- La définition de la sécurité .
- La nécessité de la sécurité .
- La sécurité physique et réseau et l'accroissement de la charte de sécurité.

Installation d'une structure

- La définition de la sécurité .
- La nécessité de la sécurité .
- La sécurité physique et réseau et l'accroissement de la charte de sécurité.

La sécurisation des utilisateurs locaux

- La stratégie d'authentification .
- La création des comptes sécurisés.
- La notion de pseudonyme utilisateur .
- Le cryptage des mots de passe et les algorithmes de chiffrement.

La sécurisation des fichiers du système de fichiers

- SSH.
- SELinux.
- NETFILTER et FirewallD.

Le chiffrement et la sécurisation des mots de passe

- L'administration des droits sur répertoires.
- Les structures de fichiers et les avantages des FS en lecture seule-sécurité de l'affichage .
- Le craqueur de mots de passe.
- Les différentes méthodes de crackage.

La sécurisation des processus et la surveillance du système

- La pratique top et strace pour surveiller les processus .
- La limitation des processus avec PAM et le contrôle des processus avec kill, nice, etc,
- La mise en œuvre et l'utilisation de la comptabilité de processus .
- La lecture des informations dans /proc avec procinfo.

La construction des firewalls

- Les fondements sur les Firewalls .
- La vérification système pré-firewall .
- Les différents types de firewalls.

Les mécanismes de sécurité

- Les mécanismes d'audit d'hôte .
- La gestion de découverte topologique d'un réseau .
- Les mécanismes de surveillance réseau .
- Les utilitaires de sécurité et de test.

Les logiciels et les services d'audit de la sécurité

- Sont-ils eux-mêmes fiables ? .
- Satan, Courtney, Gabriel, Netmon, Saint, Crack, John the Ripper, QCrack.(les plus connus).



5

JOURS

35

HEURES

CODE CPF : 208973

OBJECTIFS

Ce module doit permettre aux apprenants de tester la sécurité de leurs serveurs et de mettre en évidence les risques liés aux différents éléments

PUBLIC | PRÉREQUIS

PUBLIC

Administrateur des systèmes et réseaux, responsable IT...

PRÉREQUIS

Avoir de solides connaissances en Linux

INFOS PRATIQUES

HORAIRE DE LA FORMATION

de 9 h 00 à 12 h 30 et de 13 h 30 à 17 h 00

MÉTHODOLOGIE

PÉDAGOGIQUE

Théorie | Cas pratiques | Synthèse

MODALITÉS D'ÉVALUATION

Évaluation qualitative des acquis tout au long de la formation et appréciation des résultats

DATES ET LIEUX

Aucune session ouverte