LA HA SOUS WINDOWS AVEC FAILOVER CLUSTERING OU NETWORDK LOAD BALANCING_1603

1300 € HT (tarif inter) | REF : -RÉS1032
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Acquérir rapidement les compétences nécessaires à la sécurisation des services Internet.

2 JOURS | **14 HEURES**

PROGRAMME

Introduction

- La sécurité informatique.
- Attaques et logiciels malveillants.
- Les politiques de sécurité.
- Conduite à tenir en cas d'incident.

Cryptologie

- Les fonctions de hachage.
- Les algorithmes de chiffrement à clé publique.
- La signature numérique.
- Le protocole OpenPGP.
- Le chiffrement des systèmes de fichiers.

Protocole SSH

- Le protocole, la sécurité de type TE de SE Linux.
- L'authentification à clés publiques.
- La configuration de SSH.
- Les politiques de sécurité.
- MLS/MCS.

PKI et SSL

- Les certificats x509.
- PKI.
- SSL.
- La commande Stunnel.
- S/MIME.

Pare-feu

- Les différents pare-feu.
- Iptables.
- Tcp_wrappers.
- Xinetd.
- Squid.

VPN

- OpenVPN.
- IPSec.

La sécurisation des services

- Chroot.
- Panorama des services réseaux.
- La sécurisation des services Web : IIS, Apache,....
- La sécurisation du DNS, d'une base de données MySQL, de l'e-mail.
- La sécurisation d'un serveur : les journaux de bord.

OBJECTIFS

Connaître les moyens permettant de sécuriser les réseaux "IPTables", Firewall, Proxy, ID Savoir identifier et limiter les risques liés à l'ouverture des services Internet Utiliser des outils de surveillance à distance

PUBLIC | PRÉREQUIS

PUBLIC

Techniciens informatique, techniciens réseaux Techniciens d'exploitation, techniciens de maintenance…

PRÉREQUIS

Connaissance de la structure matérielle et logiciel d'un ordinateur Connaissances de base d'un réseau TCP / IP

INFOS PRATIQUES

HORAIRES 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