Sécurité des Architectures Linux

LE PUBLIC

Expert sécurité Systèmes, administrateurs et ingénieur sécurité des systèmes Linux.

LES OBJECTIFS

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

VOTRE FORMATION

DURÉE : 5 JOURS

35 heures

PROCHAINE SESSION :

1, 2, 3, 9 et 10 juillet 2020

LIEU : En distanciel

PRIX : 1 495 €

net de taxes

PRÉ-REQUIS

Connaissances de l'administration d'un serveur et des composants d'un environnement Linux.

RESSOURCES

- Support de cours
- 70% d'exercices pratiques

MODALITES

Formation 100 % à distance

De 4 à 16 participants

9h –17h30

Financement éligible au FNE Formation pour tout salarié d'entreprise en activité partielle

VOTRE CONTACT :

Andrea FALLOURD
Conseillère en formation
06 74 51 44 97
afallourd@itescia.fr

ITESCIA - Campus de Pontoise
8 rue Pierre de Coubertin
95300 PONTOISE

www.itescia.fr

VOTRE PROGRAMME

La sécurité informatique est devenue une préoccupation essentielle des entreprises et donc des responsables informatique.

Cette formation permet aux participants d'acquérir les connaissances et compétences nécessaires pour sécuriser les serveurs et les Infrastructures Linux.

Les enjeux de la sécurité

Les attaques, les techniques des hackers

Panorama des solutions et des guides de durcissements

Guides et référentiels pour définir une politique de sécurité

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

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

Les bibliothèques PAM

L'architecture du système PAM, les fichiers de configuration

L'étude des principaux modules

Le système SELinux ou la sécurité dans le noyau

L'architecture du système SELinux

Modifier les règles de comportement des exécutables

Les principaux protocoles cryptographiques en Client/Serveur

OpenSSL

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

Les pare-feux

Panorama des techniques pare-feux

L'architecture Netfilter/Iptables, la notion de chaine, la syntaxe d'iptables

Mise en place d'un routeur filtrant, du masquerading et d'un bastion avec iptables

Le proxy SQUID

La Sécurisation des applications

Principes généraux

Sécurisation du Web, d'email, du DNS, du FTP

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 travaux pratiques seront réalisés sur la plateforme d'entrainement **SECURITY DOJO** unique en son genre.

Les scénarii de LABs de SEC-DOJO sont tirés de cas réels avec des vulnérabilités récentes et d'actualité.

Avec les LABs de Sec-Dojo, pour monter l'infrastructure nécessaire aux travaux pratiques, vous n'avez ni à télécharger des iso, ni à installer, ni à configurer, ni à paramétrer et ni à déboguer. Vous êtes directement au cœur du sujet « la sécurité ».