

GESTION DE LA SÉCURITÉ SOUS LINUX

- ▶ **Objectif** Cette formation doit permettre aux participants de comprendre la nécessité et les exigences de la sécurité au niveau du système et du réseau. Elle leur apportera le bagage nécessaire à la mise en œuvre de la sécurité dans le cadre des systèmes Linux et des réseaux TCP/IP.
- ▶ **Opérateurs** BRUXELLES FORMATION MANAGEMENT & multimediaTIC et STERIA
- ▶ **Pré requis**
 - ▶ Diplôme de l'enseignement universitaire ou supérieur ou au minimum deux années réussies
 - ▶ Connaissances de base en informatique
 - ▶ Anglais technique
- ▶ **Sélection** Une fois par an
- ▶ **Inscription** Toute l'année lors des séances d'information de BRUXELLES FORMATION MANAGEMENT & multimediaTIC.
- ▶ **Durée** 4 mois
- ▶ **Stage** 3 mois (facultatif)
- ▶ **Certification(s)** Attestation de réussite
- ▶ **Débouchés** Administration de systèmes et réseaux (administrateur Linux / Unix, spécialiste réseau)



Programme

Concepts généraux

- Introduction - Pré requis.
- Télécommunications et réseaux :
Introduction aux techniques de transmission et aux réseaux
- Réseaux *TCP/IP* :
Architecture, adressage et protocoles *TCP/IP*.

Systèmes Linux

- Utilisation de Linux :
L'environnement Linux. Dialogue avec le système : commandes et procédures (*scripts*) *Shell*. Manipulation du système de fichiers et des fichiers.
Gestion de l'environnement utilisateur. Étude approfondie de la notion de système de fichiers.
- Administration de Linux :
Particularités des systèmes Linux. Gestion des utilisateurs, de la sécurité, des ressources et des tâches sur un système Linux.

Sécurité

- Risques et menaces *TCP/IP* :
Définition des différents types d'attaques liées aux protocoles *TCP/IP* (*DOS*, *man in the middle*, ...).
- Architecture de sécurité :
Définition d'une architecture de sécurité. Mise en œuvre d'un *firewall*, d'un proxy serveur et de *DMZs* (zones démilitarisées).
- Sécurité *TCP/IP* :
Sécurisation des accès aux réseaux étendus. Sécurisation des réseaux sans fils (*WIFI*, *WEP*).
- Sécurité Linux :
Sécurisation d'un serveur Linux au niveau local et au niveau réseau.
- Sécurité en environnement *Open Source* :
Les solutions *Open Source* pour la sécurité (*firewalls*, proxys anti-virus, *IPSec*, certification et détection d'intrusions).
- Sécurité des données :
Infrastructures à clé publique (*PKI*). Sécurité du transport des données (*SSL/TSL*, *SSH*). Technique d'authentification des utilisateurs. Outils et techniques de défense contre les logiciels malveillants.
- Audit sécurité et exploitation :
Mesure de la sécurité : définition, outils et techniques. Supervision et administration de la sécurité.

Ateliers

- Les cours théoriques accompagnés d'exercices ciblés alterneront avec de nombreux ateliers au cours desquels les notions acquises seront mises en pratique dans le cadre d'étude de cas complets.

