Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

☐	Définir une stratégie d'administration au réseau
☐	Utiliser des commandes systèmes pour observer le fonctionnement des systèmes
☐	Utiliser des outils Open Source d'administration : SmokePing, Munin, SNMP, MRTG, Nmap, AIDE et Nagios

Public concerné

Ce cours s'adresse aux administrateurs de systèmes et réseaux d'entreprise.

Prérequis

Connaissances de base des réseaux TCP/IP et de la sécurité.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant [ce test](#).

Durée de la Formation : 2 Jours (14 heures)

Prix de la Formation : 2500 euros TTC

Méthodes et moyens pédagogiques

Travaux pratiques

Echanges, partages d'expériences, démonstrations, travaux dirigés et cas pratique. Usage des commandes systèmes de base et des outils Open Source.

Méthodes pédagogiques

Pédagogie active basée sur des exemples, des démonstrations, des partages d'expériences, des cas pratiques et une évaluation des acquis tout au long de la formation.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Principes de l'administration des systèmes et des réseaux

- Que surveiller ? Utilisation des ressources systèmes. Système de fichiers. Utilisateurs. Trafic réseau. Routeurs.
- Quels moyens, quels outils ? Outils de base. Commandes systèmes, scripts routiniers. Journaux systèmes.
- Logiciels supplémentaires. Observateurs de réseaux.
- Outils SNMP. Audit de systèmes de fichiers. Scanners réseaux.

Travaux pratiques

Echanges. Définition d'une stratégie d'administration.

2 Déploiement d'un réseau TCP/IP et Linux

- Rappels sur l'architecture TCP/IP : protocoles et services. Adressage et routage.
- Classes d'adresse et masque de réseau.
- Fonctionnement général du routage et des routeurs. Configuration des systèmes. Configuration des routeurs.
- Simulateur de matériel réseau (routeurs, commutateurs) : Packet Tracer.
- Déploiement des services réseaux. Serveurs FTP, Web et DNS. Protocoles de routage. Stratégie d'administration.

Travaux pratiques

Installation d'un réseau d'entreprise : configuration de systèmes et de routeurs. Adaptation de la stratégie d'administration au réseau.

3 Commandes de base pour observer le fonctionnement des systèmes

- Observation des processus et des ressources utilisées. ps, lsof, df, du.
- Observation des utilisateurs. w, who, whodo, last.
- Analyse des services réseaux actifs. Netstat.

Travaux pratiques

Utilisation des commandes de base et pour le monitoring.

4 Outils Open Source d'administration

- Observateur de réseaux : Wireshark. Fonctionnement. Création de filtres d'affichage. Analyse de traces Wireshark.
- Scanners de réseaux : Nmap et Nessus. Qu'est-ce qu'un "scanner" ? Analyse locale. Analyse réseau.
- Audit des systèmes de fichiers : AIDE (Advanced Intrusion Detection Environment).
- Nagios, une solution complète pour le monitoring des réseaux, des serveurs et des applicatifs.
- Autres outils d'administration Open Source. Xymon (Big Brother, Hobbit).

Travaux pratiques

Configuration et utilisation de Wireshark, SmokePing, Munin, SNMP, MRTG, Nmap, AIDE et Nagios.
Présentation de Xymon (Big Brother, Hobbit).

5 Autres techniques et outils de sécurité

- Filtres sur les routeurs et les systèmes. Pare-feu.
- IDS (Intrusion Detection System). Chiffrement et certificats numériques.