



Référence : STC - LPI - 202

5 jours - 35h

Linux LPI 202

NIVEAU UTILISATEUR

Découverte

Initiation

Maîtrise

Expertise



Informations Coursus

Pré-requis

Durée : 35 heures - 5 jours

Certification préparée : Linux LPI 202

Durée de la certification : 120 minutes

Public : Ingénieur système, Administrateur, Architecte

- Avoir suivis le cursus LPI 201 ou avoir une très bonne maîtrise son contenu.

Contenu de la formation

Configuration réseau

- Configuration de base du réseau (filaire et sans fil)
- Configuration avancée du réseau et dépannage (Serveur OpenVPN, monitoring, etc.)
- Rappel sur le Troubleshooting réseau

DNS

- Configuration de base de BIND 8 et 9
- Créer et gérer des zones DNS
- Sécuriser un serveur DNS

Services web

- Mettre en place un serveur web
- Gérer un serveur web (OpenSSL, ...)
- Mettre en place un serveur proxy (squid)

Messagerie & Forums

- Configuration des listes de diffusion
- Utiliser un serveur de messagerie
- Gérer le trafic de sa messagerie
- Configurer un serveur de news

Gestion des clients réseau

- Configuration d'un serveur DHCP
- Configuration d'un serveur/client NIS
- Configuration d'un serveur LDAP
- Authentification avec PAM

Sécurité du système

- Configurer/Sécuriser un routeur avec Linux
- Sécuriser un serveur FTP
- Configuration avancée de Secure Shell (OpenSSH)
- TCP_wrappers
- Kerberos V
- Audit et tâches de sécurité (IDS, Scan, ...)

Compétences acquises/Objectifs

Vous serez capable de :

- Manipuler et configurer tout type d'interface réseau.
- Sécuriser des services réseaux (FTP,...)
- Centraliser/Authentifier des comptes avec LDAP, NIS, Kerberos, PAM
- Mettre en place un serveur de messagerie, des listes de diffusions
- Faire de l'audit sur le réseau, les services, la sécurité
- Gérer des services DNS, DHCP, Proxy (Squid)
- Mettre en place un serveur Web sécurisé

Travaux pratiques

- Configurer d'un réseau sans fil WPA et analyser les trames ARP, les connexions, ...
- Mise en place d'un tunnel VPN avec OpenVPN
- Configurer/Sécuriser des zones DNS avec plusieurs serveurs Bind 9.
- Cas pratique d'un serveur Web sécurisé (php,perl,...) avec proxy filtrant.
- Cas pratique d'un serveur de mail postfix avec outils pour alerter, filtrer les messages et d'une liste de diffusion
- Mise en place d'un serveur DHCP
- Cas pratique d'une authentification PAM avec LDAP et Kerberos V.
- Mise en place d'un routeur sécurisé avec accès par le protocole SSH.
- Cas pratique d'un serveur FTP sécurisé (SSL, TCP_Wrappers, iptables,...)
- Mise en pance d'une solution d'audit de sécurité.