# Formation Sécuriser son infrastructure réseau sous Linux

## Objectifs de la formation Sécurité Linux Réseaux

A l'issue de cette formation Sécurité Linux Réseaux vous saurez configurer les mécanismes de sécurité réseau de Linux.

## À qui s'adresse cette formation ?

**Public :**

Cette formation sécurité Linux réseaux s'adresse à toute personne souhaitant sécuriser les accès à un système Linux

**Pré-requis :**

Une bonne connaissance de l'administration des systèmes Unix/Linux et des réseaux TCP/IP est nécessaire.

# Contenu du cours Sécurité Linux Réseaux

## Introduction

Le besoin, définition du D.I.C.

Les attaques possibles

Evaluation des risques

Méthodes de protection

## Les ports de niveaux 5

Rappels sur la notion de port

Les ports UDP et les ports liés au réseau

Exemples de trames

## Outils de captures réseau

Les analyseurs de trames : tcpdump, wireshark

Travaux Pratiques :

Mise en œuvre de tcpdump, options usuelles, et possibilités de filtrage

Installation de Wireshark, capture et analyse de paquets

## Outils de Diagnostic

Scanners de ports, outils d'audit externe, et d'audit interne

Exemples de nmap, hping, sniffit...

## Audit réseau

OpenVAS (Opensource Vulnerability Assessment Scanner) : principe de fonctionnement, installation

Travaux Pratiques :

Réalisation d'un audit réseau avec openVAS

## Sécurisation des accès réseau

Protection de services réseaux au travers de xinetd
Les tcp-wrappers: telnet, tftp, snmp, ftp, pop3s, imap4s
Les contrôles d'accès :Étude des fichiers /etc/hosts.allow et /etc/hosts.deny
Les accès réseaux : sftp, les r-commandes (rlogin, rsh)
Sécurisation des transferts de fichiers avec vsftp
Présentation d'openSSH

Travaux Pratiques :

Configuration du serveur et du client pour la mise en place d'un tunnel X11 et ssh
Sécurisation http (apache) : lors de l'exécution des processus (directives user et group), portée des balises, restriction d'accès par méthode : balise Limit, LimitExcept, le fichier .htaccess : autorisation ou restriction d'accès
Authentification HTTP
Création d'utilisateurs avec htpasswd

## VPN , tunnels, iptables

Définitions : DMZ, coupe-feux, proxy
VPN et tunnels
Principe de fonctionnement
Présentation des tunnels chiffrés

Travaux Pratiques :

Mise en œuvre de stunnel pour sécuriser une messagerie smtp

Présentation d'openVPN

Travaux Pratiques :

Installation, configuration, tests de connexion, création d'un tunnel sécurisé par clé statique

Certificats : SERV et CLT

Pare-feux : les iptables, le filtrage de paquets, définition d'une politique de sécurité

Travaux Pratiques :

Mise en place des iptables

Traduction d'adresse, traduction de ports

Architecture avec pare-feux et tunneling

## Proxy Squid

Présentation, principe de fonctionnement

Architecture, hiérarchie de serveurs cache

Exemple d'utilisation, systèmes d'exploitation concernés, logiciels complémentaires

Mécanismes de configuration manuelle, automatique

Scripts d'auto-configuration, filtrage suivant DNS, par protocole

Clients en mode texte,r obots

Installation dans le navigateur

Principe et syntaxe des ACL

Optimisation de l'utilisation du serveur

Restriction d'accès par hôte, par réseau, par plage horaire, par jour, par site

Mise en cache des données

Méthodes d'authentification