



Sécurité apache

RS124

Durée: 2 jours

Public :

Toute personne souhaitant sécuriser un serveur web à base d'apache.

Objectifs :

Comprendre les mécanismes de sécurité du serveur web apache et savoir les mettre en oeuvre. Ce module s'appuie sur des travaux pratiques.

Connaissances préalables nécessaires :

Il est demandé aux participants de connaître le fonctionnement de base du serveur web Apache.

Programme :

Rappels

Fonctionnement du serveur Web Apache.
Les points essentiels de la configuration.

Atelier : installation sur la base d'une configuration exemple.

Principe, le rôle des modules.

Sécurité

Présentation des différents points à sécuriser.
Exécution des processus.
Rôles des directives User et Groupe.
Limitation de l'accès à des répertoires, fichiers ou URL.
Portée des balises, expressions rationnelles.
Octroi de capacités.
Restrictions d'accès réseau par noms de domaine, par adresses IP, par méthode Http

Atelier : exploitation des failles d'un serveur apache et sécurisation au niveau des processus, répertoires, accès réseau, ...

Authentification HTTP : mise en oeuvre.
Sécurité avec SSL et HTTPS : principe et configuration par défaut.
Certificat et clé du serveur.

Atelier : Génération de clés SSL.



— Phirio —

Authentification avec OpenLdap

Architecture avec un annuaire ldap.
Configuration dans le fichier httpd.conf

Atelier : mise en oeuvre authentification simple, filtrage d'utilisateurs

Outils d'audit et d'analyse

Analyse des flux réseaux.
Le principe des traces, les informations disponibles dans les captures de trames.

Atelier : traçage des flux réseaux avec wireshark

Atelier : audit de sécurité avec OpenVas

Atelier : étude des fichiers journaux : présentation des différents fichiers de logs disponibles