

SÉCURITÉ LINUX

CODE STAGE : AS913

OBJECTIFS

Disposer de l'ensemble des fondamentaux nécessaires à la sécurisation de ses réseaux grâce à Linux : firewall, filtrage, ...

DURÉE

5 jours

PUBLIC

Architectes réseaux, administrateurs système et réseaux, responsables de parcs informatiques.

PRÉ-REQUIS

Il est nécessaire de posséder une première expérience d'administration de Linux ou d'avoir suivi le stage Linux : Administration

PROGRAMME

1. SENSIBILISATION A LA SECURITE

Enjeux de la sécurité des réseaux et des données

Politique de sécurité

Typologie des attaques

Noyau

Services essentiels (DNS, WEB, Mail, FTP)

Autres logiciels (ICP, IE, ...)

Postes clients

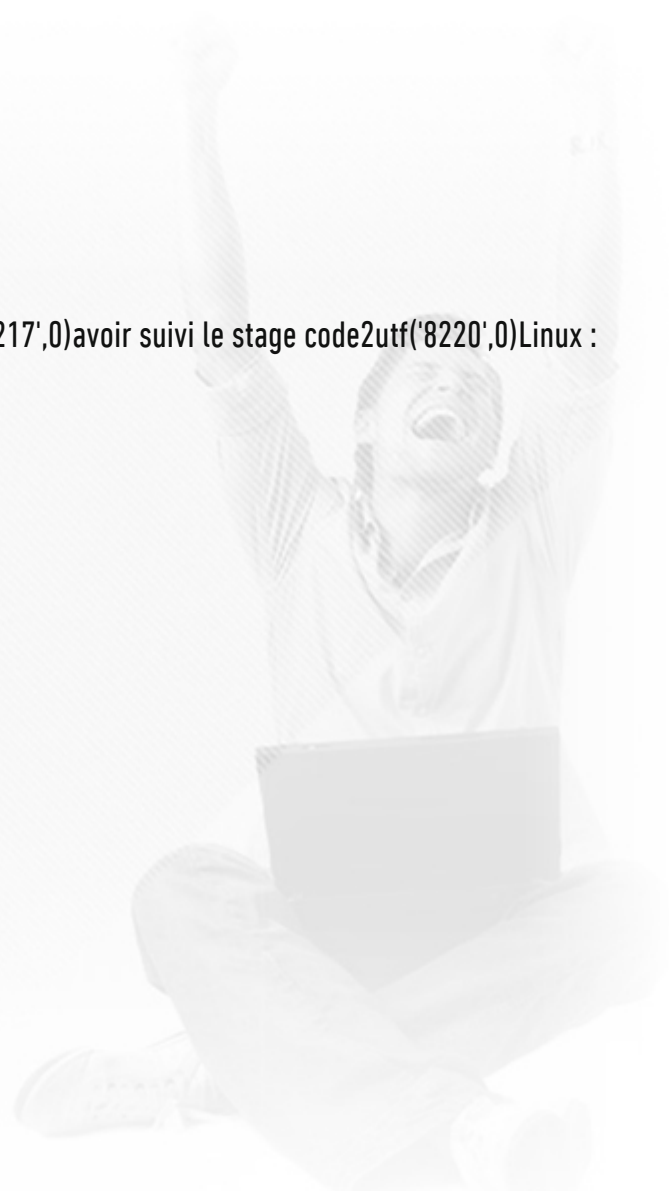
2. SECURISATION D'UN SERVEUR

La sécurité du système

Les services

Audit

SSH



Les enjeux de SSH

Les algorithmes (RSA1, RSA2, DSA)

Les solutions existantes : clients et serveurs

Mise en place du client et du serveur

Les transferts de fichiers

Utilisation avancée (intégration de script ssh_agent)

Les faiblesses

3. PROXY

Définition et fonctionnalités

4. SQUID

Filtrage : SQUID_GARD

5. FIREWALL

Les enjeux

Les protocoles

Les solutions existantes

Cas pratique : Iptables

Les outils : FWBuilder, GuardDog

Audit: vérifier les solutions mises en place

