Compte rendu de réunion
Prototype EXTRANET

Notes de réunion – procédure à suivre pour le développement du prototype pour le projet EXTRANET.

Scope du projet

L'objectif est de créer un prototype du serveur qui va héberger les sites. Pour ça, il faut reprendre les arborescences de fichiers qui simulent l'arborescence des sources sur le serveur. Pour l'instant le développement n'a pas été fait, ça viendra plus tard. Pas besoin non plus de mettre en place le DNS.

1. Le serveur

- Préparation d'une machine virtuelle, capacité minimale 1 CPU, 1 024 ou 2 048 Mo de mémoire, 10 Go d'espace disque suffiront.
- Deux pattes réseaux :
    - une sur le 192.168.10.0/24 pour l'interne ;
    - une pour simuler l'externe en 150.10.0.0/16, par exemple.
- Installation d'une distribution Debian ou Ubuntu, mais en version minimale, pas d'environnement de bureau. On est ici sur un projet serveur.

2. Le service web

- Installation du serveur HTTPD d'Apache. À faire avec les packages de la distribution, inutile de compiler la dernière version.
- Création de deux virtual hosts :

    - extranet.rainbowbank.com ;
    - admin.rainbowbank.com.
- Les deux vhosts doivent référencer deux arborescences de sources différentes. Recommandation : créer deux répertoires dans le /var/www (extranet.rainbowbank.com et admin.rainbowbank.com, par exemple).
- Le vhost extranet doit être accessible sur la patte réseau publique, le vhost admin uniquement sur la patte privée.
- Changement du port d'écoute pour le vhost admin en 5501 pour HTTP et 5502 pour le HTTPS, par exemple.
- Génération d'un certificat auto-signé wildcard pour les deux vhosts. Pour ça, il faut utiliser les données de l'entreprise et l'adresse mail admin (FR, ILE DE FRANCE, PARIS, RAINBOW BANK, DIRECTION INFRASTRUCTURE ET LOGISTIQUE et admin@rainbowbankcom).
- Mise en place d'une redirection forcée des requêtes entrantes HTTP vers HTTPS pour les deux vhosts.
- Attention à créer deux fichiers de traces d'accès, un pour chaque vhost. Il est possible de garder le même fichier de trace pour les erreurs.
- Configurer les droits d'accès sur les répertoires sources du service HTTPD, il faut qu'ils soient sécurisés au maximum.
- Il faut cependant prévoir les droits d'écriture pour le vhost extranet dans le répertoire PDF, car les utilisateurs vont pouvoir charger des fichiers directement depuis le site.

→ Tester cette partie 2 également avec NGINX.

3. Le service FTP

- L'idée ici est de rendre accessibles les répertoires des sources des sites aux personnes qui en ont besoin.
- Les futurs développeurs vont avoir besoin d'accéder aux répertoires des codes sources des deux vhosts.

- Les graphistes doivent uniquement accéder aux répertoires des images des deux vhosts.
- Il faut bien évidemment refuser les connexions anonymes.
- Recommandation : créer des groupes Linux pour gérer ces droits et inventer deux comptes nominatifs de test : un pour un développeur et un pour un graphiste.
- Mise en place d'un cloisonnement via un chroot ou un jail sur ce service, pour bien le sécuriser.
- Le service FTP doit être uniquement accessible sur la patte privée.

4. Le filtrage

Un filtrage IP avec netfilter doit être appliqué sur le serveur en laissant passer le minimum de protocoles nécessaires sur les deux pattes réseau (il est possible de garder le flux SSH sur la patte interne pour l'administration du serveur).

5. La prévention sur la sécurité

Il faut mettre en place les mesures préventives suivantes en termes de sécurité :

- Utiliser des modules et des paramètres de configuration qui permettent de se prémunir contre les attaques DDoS ou slow connections.
- Appliquer des configurations Fail2Ban qui permettent d'ajouter automatiquement des règles de filtrage dans netfilter sur 3 mauvaises tentatives de connexion FTP d'affilée, et sur 3 requêtes sur un fichier de l'arborescence des sites (temps de ban de 5 minutes, seulement pour vérifier que ça fonctionne).