Administration système et réseaux II

Rapport Sécurité

Groupe 2.

BOHYN gauthier

Hermant THIbaut

hanquet brian

# Rapport Sécurité (Mail)

## Serveur Web - DNS

Nous allons utiliser le Protocole HTTPS. (Nous devrons valider un certificat de sécurité). *Plus de sécurité avec le protocole HTTPS, toutes les données sont chiffrées.*

Nous ne l’avons pas encore installé mais cela est prévu prochainement.

Nous allons utiliser premièrement Fail2Ban pour sécuriser les serveurs.

### Risques

* *Le certificat de sécurité n’est pas encore fait (HTPS)*

## Sécurisation sur les VPS

*Nous avons créé un nouvel utilisateur pour ne plus se connecter en super-utilisateur. Ensuite nous avons généré une clé publique et clé privée, afin de pouvoir les protéger à l’aide d’une phrase de sécurité.*

* *Mises à jour de mot de passe par exemple régulièrement* 
  + *Permet de garder une sécurité si perte ou piratage de mot de passe*
* *Création d’un nouvel utilisateur admin* 
  + *Permet de ne pas se connecter directement avec au super-utilisateur (Root) lors de la connexion au VPS.*
* *Installation de Fail to Ban*
  + *Permet de se protéger contre les tentatives d’intrusions*

### Risques

* *Connexion encore possible sur le Root car nous n’avons pas encore désactivé l’accès au VPS en SSH pour cet utilisateur.*

## Serveur Mail

*Nous pouvons éventuellement utiliser un certificat SSL pour plus de sécurité pour les mails, mais nous ne l’utilisons pas encore personnellement.*

*Bien évidemment, les mots de passes utilisés devront être complexe à trouver pour augmenter la difficulté de le trouver.*