Administration système et réseaux II

Rapport Sécurité

Groupe 2.

BOHYN gauthier

Hermant THIbaut

hanquet brian

# Rapport Sécurité (VoIP)

## 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 Fail2Ban pour sécuriser les serveurs.

### Risques

*Les serveurs web peuvent toujours faire l’objet d’attaque que ce soit par des virus ou par des pirates experts. Les conséquences sont constituées généralement par des fuites d’informations personnelles et par l’exploitation des données personnels de l’utilisateur. Une mauvaise configuration de sécurité peut produire une faille lorsque les serveurs d’application, serveurs web, serveur de base de données, … N’ont pas de configuration sécurisée correctement établie et déployée. Soit, l’Entreprise doit toujours rester vigilant pour éviter d’être victime d’une quelconque atteinte.*

## 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 copiage de mot de passe par une autre personne.
* Création d’un nouvel utilisateur admin
  + Permet de ne pas se connecter au super-utilisateur (Root) lors de la connexion au VPS.
* Installation de Fail to Ban
  + Permet de se protéger contre les tentatives d’intrusions. Fail to Ban bloque l’accès après plusieurs fausses connections
* *Installation de UFW*
  + *UFW (Uncomplicated Firewall) est le pare-feu installé par défaut d'Ubuntu, un outil de configuration simplifié en ligne de commande sous GNU/Linux.*

### Risques

* *Attaques de coupe*

*Une machine cliente pourrait éventuellement être la cible d’une attaque dans le réseau. Un intrus pourrait exploiter des bugs ou des erreurs pour lancer une attaque pirate. Dans le pire des cas, le VPN pourrait être détourné et contrôlé par un tiers. Le trafic pourrait être intercepté, supprimé ou modifié.*

* *L’authentification*

*Par défaut, un VPN ne fournit pas une authentification forte aux utilisateurs. Une connexion VPN ne doit être établie que par un utilisateur authentifié, pour restreindre l’accès aux seuls utilisateurs autorisés.*

* *Infection virus*

*Un réseau de connexion peut être compromis si le client est infecté par un virus. Si un virus ou spyware infecte un ordinateur client, il est possible que le mot de passe du VPN soit divulgué à un attaquant. Si le réseau est infecté par un virus, ce dernier peut être propagé à d’autres réseaux. Aujourd’hui cependant, des protections anti-virus efficaces sont mises en place.*

## Serveur Mail

*Nous pouvons éventuellement utiliser un certificat SSL pour plus de sécurité pour les mails.*

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

### Risques

* *Il peut avoir un risque de spam ! Nous pouvons par la suite faire la démarche pour empêcher ce spam et détecter les adresses mails concernés.   
  Un pirate peut se servir de cette faille pour se faire passer pour vous ou un membre de votre organisation afin de soutirer des informations à vos clients/correspondants.  
  A l’évidence, l’émission de messages non sollicités sous votre nom peut nuire à votre image ou l’image de votre entreprise.  
  Cela peut s’avérer également catastrophique d’un point de vue technique car votre boîte mail peut se retrouver inondée de milliers de messages d’erreurs si une attaque de spam est menée avec votre adresse. Ce type d’attaque est particulièrement difficile à bloquer car les e-mails parviennent souvent d’un grand nombre de serveurs différents et cela peut mener un serveur de messagerie à la panne complète.*

*🡪 Pour se protéger de ces risques, plusieurs systèmes d’authentification du nom de domaine de l’expéditeur d’un message ont été créés. En voici quelques-uns :*

* + ***SPF****(Sender Policy Framework)*
  + ***Sender ID***
  + ***DKIM****(Domain Keys Identified Mail)*

## VoIP

### Risques

* Les interruptions

Les attaques peuvent impliquer des virus ou des vers susceptibles de perturber, voire de bloquer tous les services de la téléphonie IP.

* Les Spams ou SPIT (Spam over Internet Telephony ou pourriel par téléphonie Internet)

La ligne de téléphonie IP est la cible d’actions marketing indésirables

* La perte de confidentialité

La majeure partie du trafic sur un système téléphonique IP n’est pas chiffrée. Ce qui offre à un individu mal intentionné l’occasion d’écouter clandestinement et d’espionner sans trop de difficulté les conversations. Un pirate peut, non seulement intercepter et enregistrer les appels vocaux, mais peut aussi accéder au système de gestion des appels, tel que la boîte vocale, le renvoi d’appel ou l’identificateur des appelants.

* Le piratage

Ce type d’attaque consiste à s’introduire frauduleusement dans un réseau VoIP et d’effectuer une multitude d’appels non autorisés vers des numéros interurbains ou internationaux.