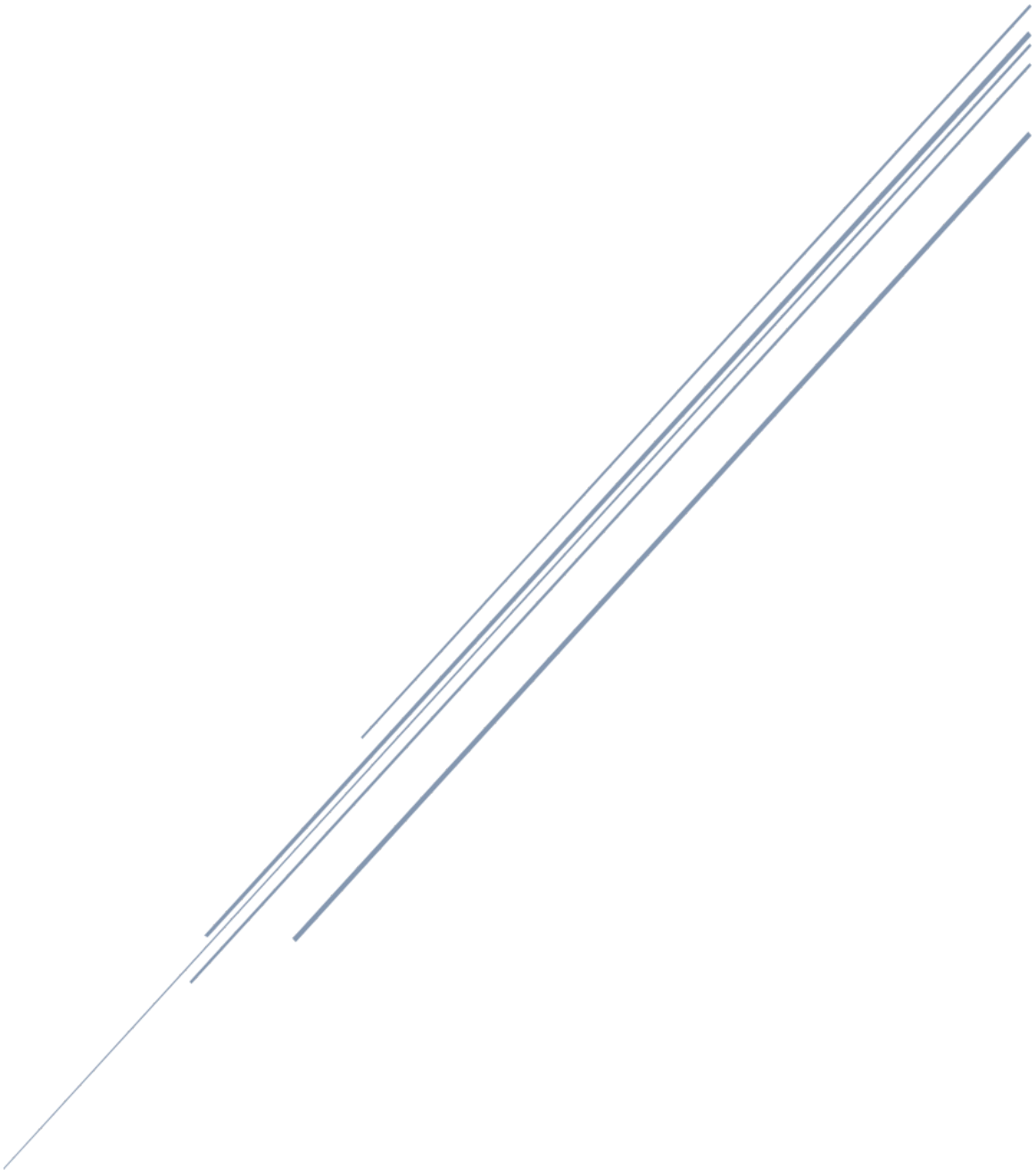
Administration système et réseaux II
Rapport Sécurité



GROUPE 2.
BOHYN GAUTHIER
HERMANT THIBAUT
HANQUET BRIAN

Rapport Sécurité

Firewall

Le Firewall permet :

- Une protection entre un réseau interne et un réseau externe.
- Un filtrage des paquets sur base du quintuplet (IP_src, P_src, IP_dst,P_dst, protocole).
- Les actions : Accept or Deny.
- L'état Firewall Stateful : Garde l'état des connexions TCP (UDP dans une moindre mesure).

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

Voici plusieurs risques d'attaque liés au DNS :

- Interception de paquets : l'auteur modifie alors le paquet pour par exemple falsifié la réponse.
- Corruption des données du serveur : pour faire du cache-poisoning ou la mise en avant d'un service commercial.
- Déni de services : généralement dû a une surcharge de serveur.

Solutions

La meilleur solution pour la sécurisation d'un DNS reste à l'heure actuelle DNSSec.

DNSSec est un protocole de sécurité qui permet la signature cryptographie des enregistrements DNS.

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.

Fonctionnement

- Première étape : Mise en place d'un canal sécurisé
- Deuxième étape : Authentification du client auprès du serveur
    - Authentification par mot de passe : ne garanti pas l'autorisation et risque de "craquage".
    - Authentification par clé public : clé déposée sur le serveur SSH ce qui permet un accès physique.

Détails

- 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.
    - Il permet d'ouvrir seulement les ports utilisé et de fermer les autres .

Risques

- Attaques de coupe

Une machine cliente pourrait éventuellement être la cible d'une attaque dans le réseau. Dans le pire des cas, le VPS pourrait être détourné et contrôlé par un tiers. Le trafic pourrait être intercepté, supprimé ou modifié.

- L'authentification

Par défaut, un VPS ne fournit pas d'authentification forte aux utilisateurs. Une connexion VPS ne doit être établie que par un utilisateur authentifié afin de 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 VPS 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

Bien évidemment, les mots de passe utilisés devront être complexes à trouver pour augmenter la difficulté.

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)

Solutions

Nous pouvons éventuellemet rajouter quelques solutions pour la sécurisation d'un serveur mail :

- Filtre anti-spam
- S/MIME : permet de signer et/ou de chiffrer des messages mail.
- PGP : logiciel de cryptographie permettant la confidentialité et l'intégrité des données.
- Proxies Mail : utile en DMZ pour isoler les serveurs mails eux-mêmes de l'internet.
- Proxy SMTP : Filtrage des spam et virus en inbound et filtrage des spam sortant en outbound.

VoIP

Concernant la sécurité des VoIp's, les mots de passe qui doivent être complexes !

```
25  [100](default_template)
26  fullname = Secretaire
27  username = secretaire
28  secret=ra5Y4CWD
29  mailbox = 100
30  context=direction
```

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
  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 difficultés les conversations. Un pirate peut, non seulement intercepter et enregistrer les appels vocaux, mais peut également accéder au système de gestions 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.