MOUGAMMADOU Zaafir

LA NOTIFICATION EMAIL POUR LA CONNEXION SSH

IMIE PARIS

Cursus : BTS SIO OPTION SISR
Entreprise : Préfecture de Police de Paris
Poste : Apprenti Technicien Support
Tuteur : Alain Rigot

REMERCIEMENTS

Je souhaite adresser mes sincères remerciements à toutes les personnes qui ont contribué au succès de mon alternance et à la rédaction de mon Projet Personnel Encadré .

Je voudrais dans un premier temps remercier Monsieur JACQUET, professeur de spécialité SISR à l'IMIE PARIS. Le mérite d'un écrit comme celui-ci appartient certes à l'auteur, mais également à celui qui l'encadre. En tant que professeur, il m'a accompagné tout au long de ma progression.

Je remercie également toute l'équipe de la DILT pour leur accueil chaleureux au sein de leur entreprise. Ils m'ont ouvert les portes de leurs univers avec enthousiasme. Le service Support IT donne une importance à chacun de ses membres avec un esprit d'équipe et de cohérence professionnelle. Grâce à eux, j'ai énormément appris de moi sur le plan personnel mais surtout professionnel.

Je suis particulièrement reconnaissant envers mon tuteur d'entreprise, Alain RIGOT et toute son équipe pour leur patience et leur disponibilité. Leur encadrement a été important tout au long de mon expérience.

Enfin, je remercie mes proches pour leur soutien et leurs encouragements. Ils ont su se rendre disponible quand cela était nécessaire.

Mon expérience au sein de cette entreprise a été un plaisir. J'ai beaucoup appris, tant humainement que professionnellement et cela m'a permis de rédiger mon Projet Personnel Encadré.

SOMMAIRE

INTRODUCTION

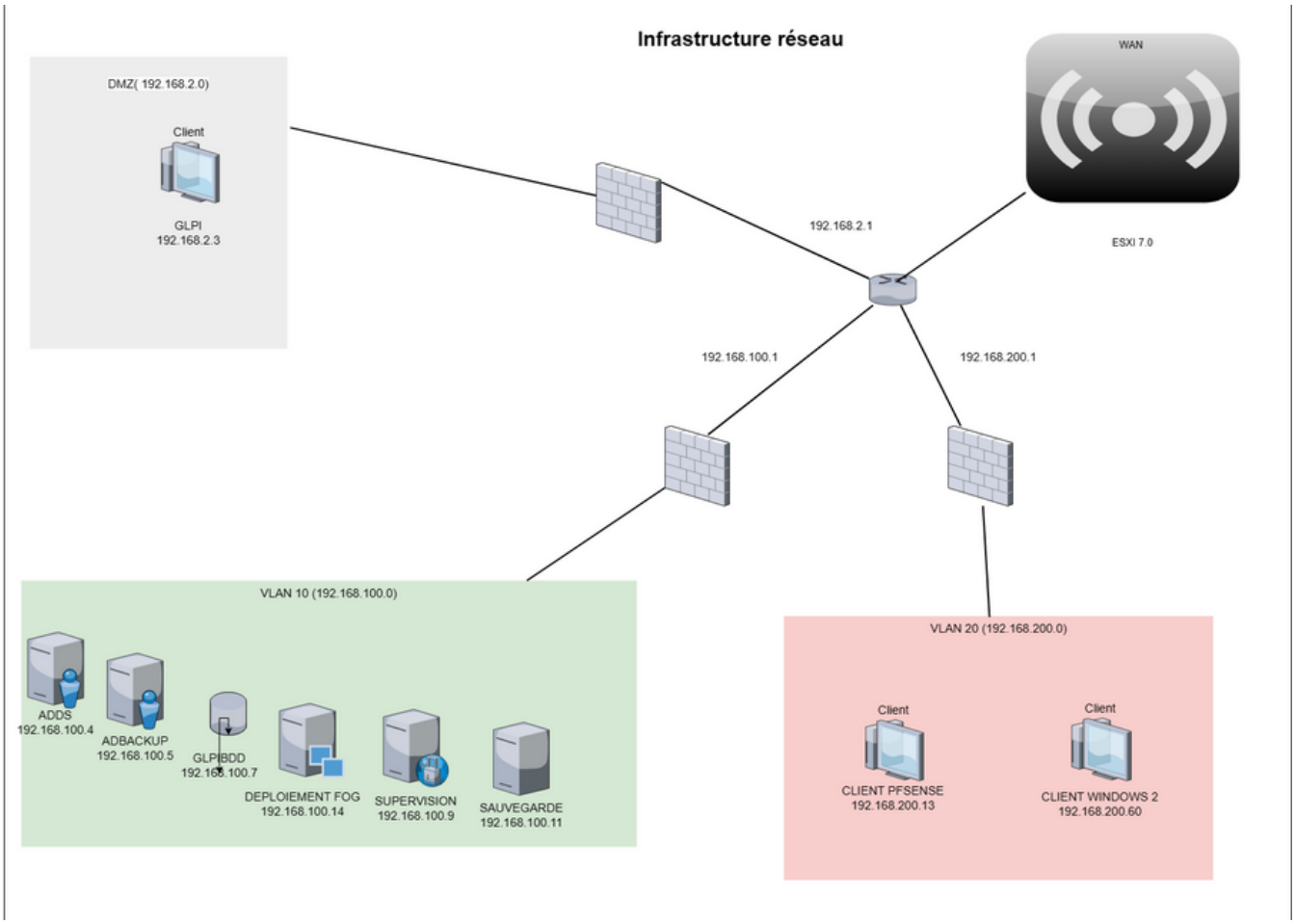
Actuellement en contrat d'apprentissage au sein de la Préfecture de Police de Paris, j'ai eu l'opportunité à travers mon expérience, mes recherches et les enseignements reçus au cours de mon BTS SIO d'approfondir mes connaissances et également de découvrir la notion de sécurité informatique.

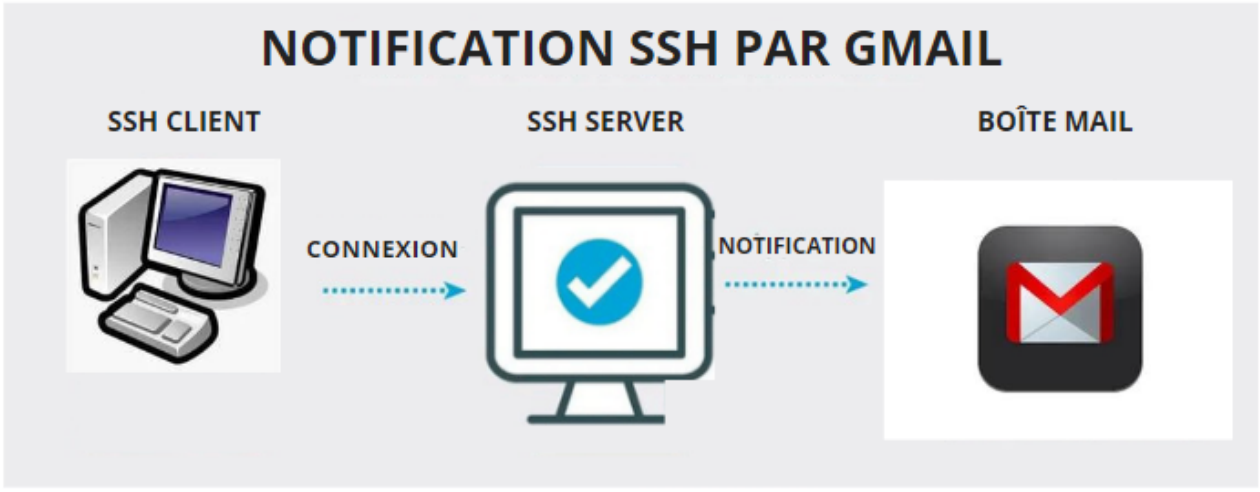
Aujourd'hui, la sécurité informatique est devenue incontournable pour toutes les entreprises souhaitant intégrer les nouvelles technologies dans leurs activités. Cette évolution technologique et plus particulièrement d'Internet et de l'informatique s'adresse désormais aux entreprises de toutes les échelles.

Dès lors, notre question de recherche s'énonce de la manière suivante : « Dans quelles mesures la MFA augmente la sécurité lors des connexions à distance ? »

Ce sujet se structure autour de trois parties distinctes. Dans un premier temps la première partie porte sur le paramétrage de la connexion SSH. Ensuite, nous mettrons en place l'authentification MFA. Enfin, dans une troisième partie, nous configurerons un serveur de messagerie afin de recevoir des notifications d'alertes lors des connexions à distance sur notre serveur.

ARCHITECTURE





La connexion SSH

SSH est un acronyme pour Secure Shell. C'est un terme général qui fait référence à plusieurs versions du protocole SSH.

Le protocole SSH exploite les normes de sécurité des services réseau d'hôtes non autorisé à travers des réseaux non sécurisés. SSH est l'un des plus grand gérant des serveurs internet dans le monde, sur les sites et notamment dans le Cloud. Ce protocole est souvent combiné avec d'autres protocole internet et permet une communication sécurisée à distance entre un poste client et un serveur. Il permet d'effectuer plusieurs tâche en amont par les administrateurs systèmes des entreprises mais aussi de streamer des vidéos en utilisant le protocole SFTP.

Ce protocole est situé sur la couche application du modèle TCP/IP utilisant le port de communication qui est le 22 par défaut. SSH est divisé en trois couches : la couche de transport , la couche d'authentification et de la couche connexion.

- La couche de transport gère le chiffrement et le décryptage des données échangées entre les deux hôtes et assure la confidentialité et l'intégrité de l'échange.

- La couche d'authentification permet d'identifier l'identité du client lors de la connexion à distance.

- La couche de connexion gère les tunnels à travers lesquels circulent les données entre les deux machine

1.1- La Sécurité générale du SSH

SSh est un protocole qui a vu le jour pour substituer les protocoles shell non sécurisés tels que Telnet ou même FTP . Cependant, l'avantage du SSH est l'utilisation d'un système de cryptage permettant d'assurer un transfert de données sécurisées entre le poste client et le serveur afin de garantir la confidentialité de l'information. Il existe trois types de méthode de chiffrement: le chiffrement symétrique , le chiffrement asymétrique et le hachage.

- Le chiffrement symétrique possède une clé secrète, qui est utilisée pour le chiffrer et pour le décryptage des connexions SSH.

- Le chiffrement asymétrique possède deux clés différentes - une paire de clés publique/privée pour le chiffrement et le décryptage. Le cryptage asymétrique permet également d'authentifier l'identité du client pour le serveur.

- La méthode de hachage transforme les informations transmises en un autre caractère unique et vérifie l'authenticité des messages.

De plus, la tunnelisation du SSH permet d'envoyer des informations non chiffré sur un réseau à travers un canal chiffré. Par exemple, un tunnel SSH peut permettre à un serveur FTP qui n'est pas chiffré de transférer des données en toute sécurité. D'autant plus, les tunnels SSH met en place un chemin sécurisé vers les VM's à travers un pare-feu et internet pour garantir l'intégrité des données.

1.2 - L'authentification par mot de passe

De nos jours, l'authentification par mot de passe est très simple. Cependant, pour mieux sécurisé cette méthode d'authentification, il faudrait privilégier les recommandations de l'ANSSI :

- Imposez une longueur minimale (12 à 16 caractères)
- 1 minuscule minimum
- 1 majuscule minimum
- 1 chiffre minimum
- 1 caractère spéciale minimum
- éviter l'utilisation d'informations personnelles

En outre, si quelqu'un tente de se connecter sans le bon mot de passe la connexion sera bloqué. C'est le failsafe.

1.3 - L'authentification par clés publique/privée

L'authentification par clés publique/privée demande des paramétrages en plus pour garantir une sécurité complète. Cette clé est générée automatiquement par l'ordinateur ce qui est beaucoup plus long qu'un mot de passe classique. Une fois la paire de clé enregistrés , le client peut s'identifier au serveur SSH. Par conséquent, si quelqu'un tente une connexion sans la bonne combinaison de clé publique/privée, la connexion sera refusée.

LA NOTIFICATION SSH PAR EMAIL

La notification SSH par email nous permet d'être notifier par email lors d'une connexion effectué sur notre serveur. Pour mettre en place ce dispositif, il faut installer "Postfix" un serveur de messagerie utilisant le protocole SMTP, sur notre système d'exploitation Linux.

3.1 - Un serveur email : "Postfix"

Pour mettre en place le serveur de messagerie , nous allons installer "Postfix", un serveur de messagerie permettant d'envoyer des mails d'alertes via des scripts bash. L'avantage avec ce serveur, c'est qu'on peut utilisé le serveur de messagerie de Google en envoyant des mails avec notre adresse Gmail personnel.

Pour l'installation de ce serveur il faudrait d'une part , mettre à jour le cache puis installez le paquet suivant :

```
┌──(root㉿kali)-[~]
└─# apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules
```

De plus, ce module est composé de plusieurs fonctionnalités tels que :

- mailutils, un gestionnaire de courriel.
- libsasl2-2, l'implémentation de l'interface de programmation Cyrus SASL.
- ca-certificates, un certificat permettant d'identifier l'identité du correspondant

Suite à l'installation du paquet "postfix mailutils libsasl2-2 ca-certificates libsasl2-modules", il faut activé le système et poursuivre avec la configuration du fichier Postfix en exécutant les commandes suivante :

```
┌──(root㉿kali)-[~]
└─# systemctl enable postfix
```

```
┌──(root㉿kali)-[~]
└─# nano /etc/postfix/main.cf
```

Une fois sur le fichier de configuration, nous devons cherchez et modifiez la ligne suivante : `relayhost =`

Par : `relayhost = [smtp.gmail.com]:587`

Cette modification permet d'indiquer que le serveur SMTP utilisé est celui de Gmail. Par la suite, il faut se rendre à la fin du fichier pour rajouter les lignes suivante :

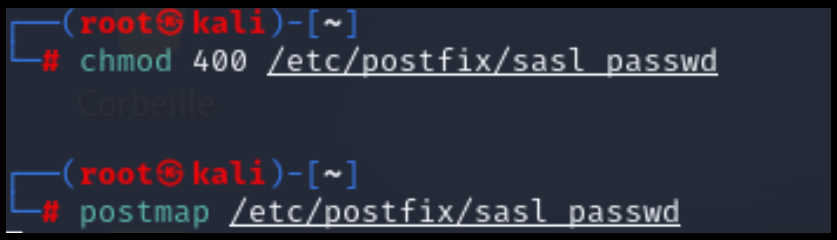
```
#Postfix

smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_use_tls = yes
```

Ces commandes ont pour objectif, d'activer l'authentification , d'indiquer l'emplacement du fichier "sasl_passwd", d'interdire le mode anonyme, d'indiquer le chemin du certificat et enfin d'activer le TLS.

Pour préciser d'où les mails arrivent sur notre boîte mail, il nous faut crée le fichier "sasl_passwd" et nous devons saisir la ligne suivante :

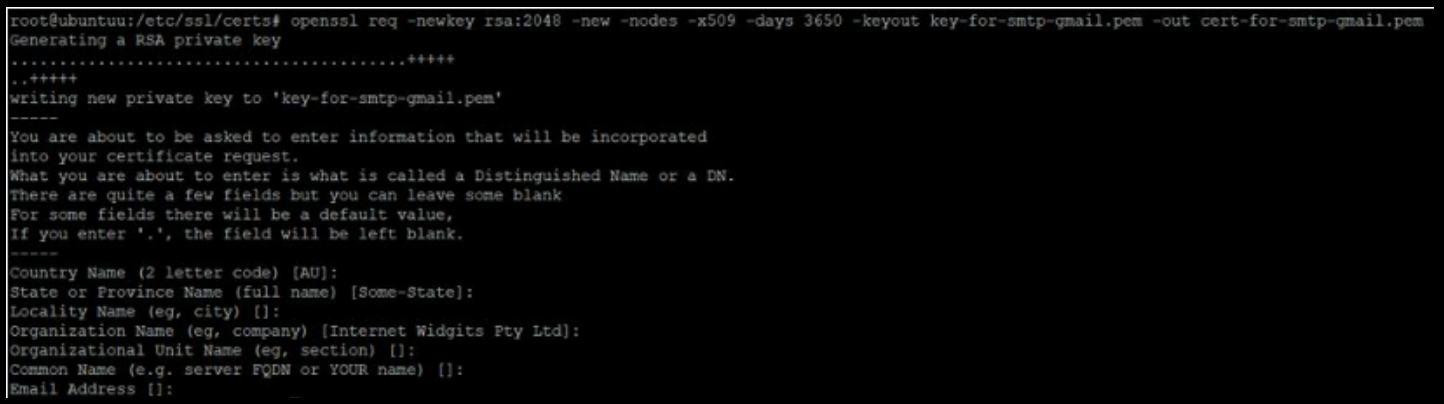
Le début de la ligne précise qu'on utilise le SMTP de Gmail qui est sur le port d'écoute 587. Ensuite, on doit saisir notre adresse Gmail ainsi que notre mot de passe d'application qui est un mot de passe nous permettant de se connecter à notre compte Gmail à partir de plateforme ou application non compatible.

Cependant, pour utiliser le fichier il lui faut attribuer les droits et puis exercer un postmap dessus afin de créer une base données.



De plus, un certificat SSL/TLS doit être créer pour pouvoir chiffré les mails envoyés afin qu'ils circulent sur le serveur SMTP en toute sécurité. Pour cela, nous allons utilisez la commande suivante et remplir les informations demandées :

```
cd /etc/ssl/certs

openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout key-for-smtp-gmail.pem -out cert-for-smtp-gmail.pem
```



Une fois le certificat généré on le redirige dans le fichier "/etc/postfix/cacert.pem" comme ci-dessous :

```
cat /etc/ssl/certs/cert-for-smtp-gmail.pem | sudo tee -a /etc/postfix/cacert.pem
```

Enfin, une fois les configurations des fichiers terminés, il faut redémarrer le service postfix, afin que tout les changements s'appliques et vérifier que celui-ci est bien activé via la ligne de commande ci-contre :

```
/etc/init.d/postfix reload
```

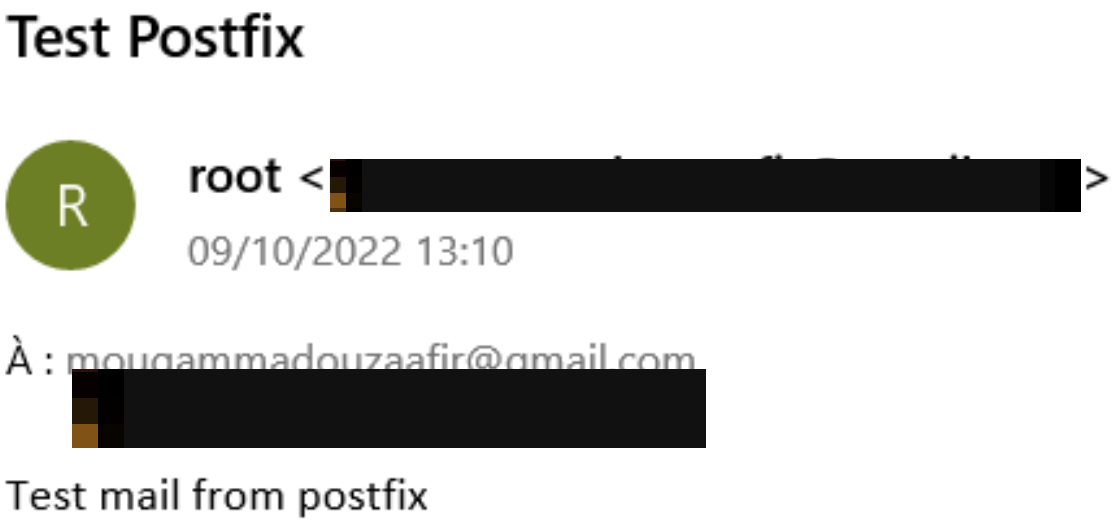
```
/etc/init.d/postfix status
```

```
root@ubuntuu:/etc/ssl/certs# /etc/init.d/postfix reload
Reloading postfix configuration (via systemctl): postfix.service.
root@ubuntuu:/etc/ssl/certs# /etc/init.d/postfix status
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
     Active: active (exited) since Mon 2021-03-29 15:03:23 CEST; 12min ago
    Process: 4450 ExecReload=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 3291 (code=exited, status=0/SUCCESS)

mars 29 15:03:23 ubuntuu systemd[1]: Starting Postfix Mail Transport Agent...
mars 29 15:03:23 ubuntuu systemd[1]: Finished Postfix Mail Transport Agent.
mars 29 15:15:45 ubuntuu systemd[1]: Reloading Postfix Mail Transport Agent.
mars 29 15:15:45 ubuntuu systemd[1]: Reloaded Postfix Mail Transport Agent.
root@ubuntuu:/etc/ssl/certs#
```

Pour tester notre configuration , nous allons exécuté la commande suivante :

```
echo "Test mail from postfix" | mail -s "Test Postfix" adresse@mail.com
```

Pour cela, il faut d'une part remplacer "adresse@mail.com" par l'adresse Gmail du destinataire et d'autre part définir l'objet du mail après "mail -s" et l'intitulé du mail après "echo".



Maintenant qu'on reçoit les mails sur notre boîte mail Gmail , nous pouvons configuré le système de notification par email le serveur SSH.

3.2 - Le fichier "pam.d/sshd"

Lors d'une authentification sur un serveur Linux, PAM le système d'authentification qu'on avait installé en amont permet au SSH de crée le fichier de configuration "/etc/pam.d/sshd" en arrière plan. Par conséquent c'est dans ce fichier qu'on déclarera le script BASH "Alerte e-mail" avec "pam_exec" un module qui nous permettra d'exécuter les commandes extérieur.

```
┌──(root㉿kali)-[~]
└─# nano /etc/pam.d/sshd
```

```
# Notification en cas de connexion SSH
session  required  pam_exec.so  /etc/pam.scripts/ssh-alert.sh
```

3.3 Script BASH "Alerte e-mail"

D'une part, le script qui nous permettra de configurer notre serveur Linux afin de recevoir des notifications par e-mail lors des connexions via le SSH est le suivant :

```
#!/bin/bash

expediteur="`hostname`-ssh@gmail.fr"
destinataire="mougammadouzaafir@gmail.fr"
objet="`hostname` - Connexion SSH"
body="<h2><b>Serveur `hostname` - Nouvelle connexion SSH</b></h2><br><b>— Hôte distant : </b>$PAM_RHOST<br><b>— Utilisateur : </b>$

if [ ${PAM_TYPE} = "open_session" ]; then
    echo "${body}" | /usr/bin/mail -r "${expediteur}" -s "${objet}" "${destinataire}" -a "Content-Type: text/html"
fi
exit 0
```

D'autre part, pour exécuter ce script nous allons crée un dossier "pam.scripts" dans lequel on crée un fichier "ssh-alert.sh" , puis on enregistre le script à l'intérieur et on l'attribue les droits.

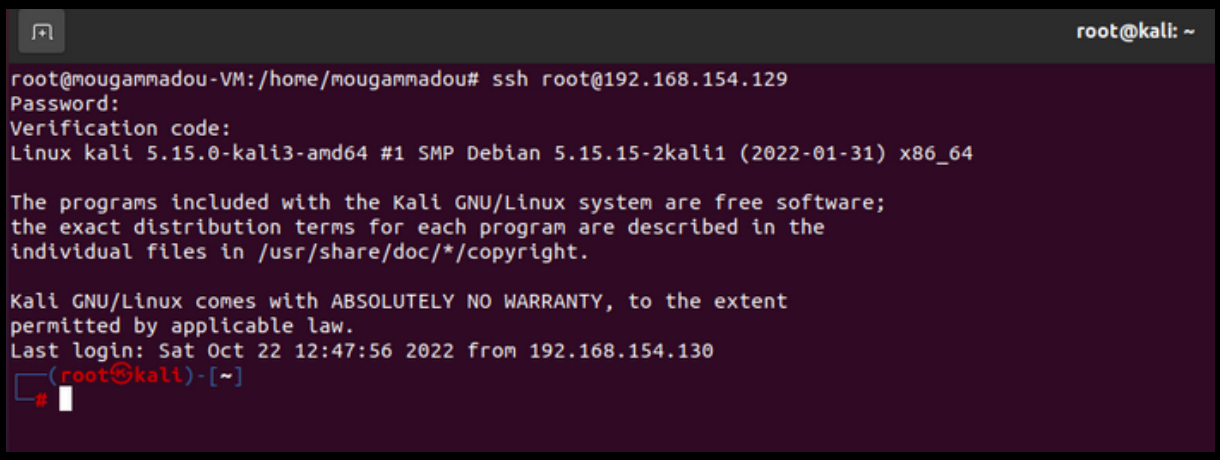
```
┌──(root㉿kali)-[~]
└─# sudo mkdir /etc/pam.scripts
```

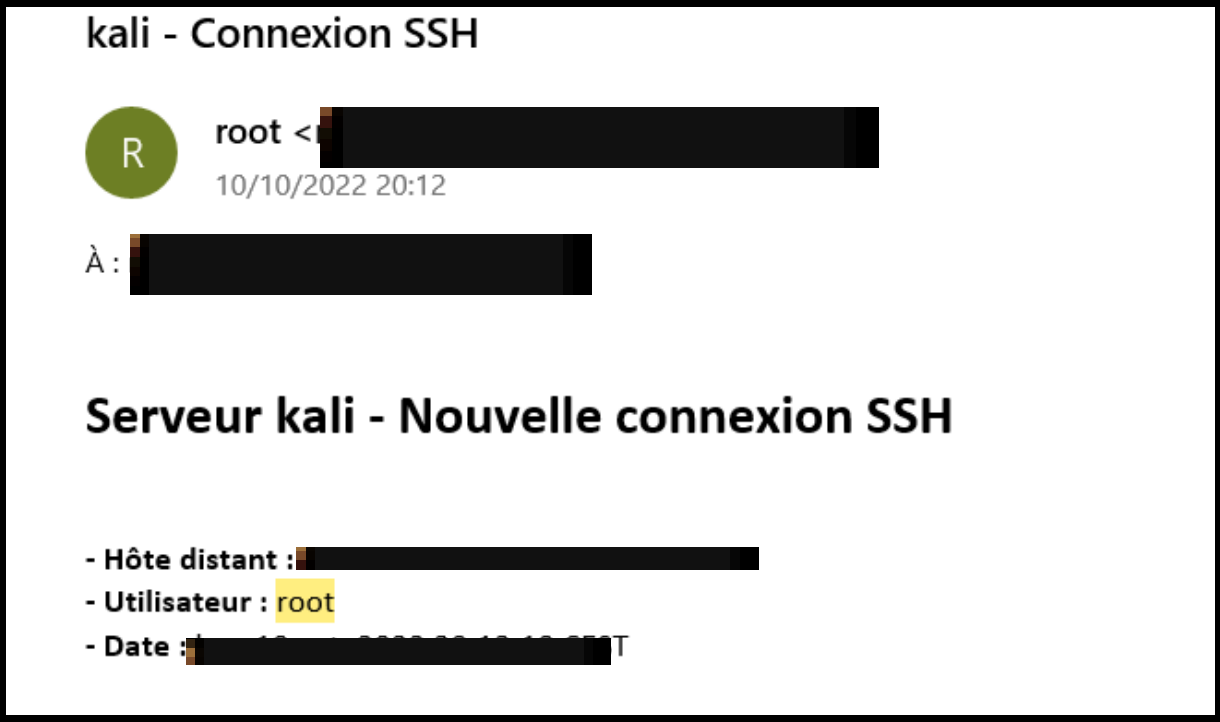
```
┌──(root㉿kali)-[~]
└─# nano  /etc/pam.scripts/ssh-alert.sh
```

```
┌──(root㉿kali)-[~]
└─# chmod 700 /etc/pam.scripts/ssh-alert.sh
   chmod +x /etc/pam.scripts/ssh-alert.sh
```

3.4 Tester la notification par e-mail

La dernière étape consiste à effectué une connexion à distance avec un poste client sur notre serveur SSH afin de recevoir un mail de notification :





On peut constater qu'on reçoit bien un mail lorsque quelqu'un tente de se connecter à distance au serveur SSH, et que cela fonctionne.

CONCLUSION

En conclusion, nous sommes aujourd'hui dans une époque où la sécurité informatique est très importante. Ce renforcement de la sécurité implique des changements incontournables au sein des entreprise car parfois le manque de protection de données peut impacter la vie personnelle et professionnelle des personnes.

L'objectif des entreprises est d'intégrer toutes les nouvelles technologies dans leurs activités pour s'adapter aux évolutions des employés et continuer à se déployer et répondre à leurs besoins donc la sécurité de leur nouveaux acquis est primordial.

Ainsi, la sécurité informatique est question d'humain et doit être accompagnée. Les ingénieurs informatique, administrateurs système, les techniciens support sont le point central de cette protection et doivent motiver les employés afin qu'ils contribuent à la performance de l'entreprise. Le facteur humain est la clé du succès pour l'évolution de la sécurité informatique.

Cependant, il est indispensable d'adapter des outils et des compétences pour sécurisé nos activités. L'entreprise doit donc avoir une bonne capacité d'adaptation en créant un réseau protégé pour inciter un travail sécurisé.

WEBOGRAPHIES

- https://www.paessler.com/it-explained/ssh
- https://www.appvizer.fr/magazine/services-informatiques/mots-de-passe/anssi-gestionnaire-de-mot-de-passe
- https://manpages.ubuntu.com/manpages/impish/man8/pam_google_authenticator.8.html
- https://www.it-connect.fr/linux-comment-activer-le-mfa-sur-un-acces-ssh/
- https://www.it-connect.fr/configurer-postfix-pour-envoyer-des-mails-avec-gmail/
- https://www.it-connect.fr/linux-recevoir-un-e-mail-lors-dune-connexion-ssh/