BEM TECH

BEM Africa

Projet de sensibilisation sur le phising.
Sous le thème de :

Simulation d’une attaque par phishing

Présenté par :

Moustapha SY

Table de matières

Table des figures

Résumé

Une campagne de phising a été simuler à l'aide de l'outil Gophish afin d'évaluer la réaction du personnel face à un email frauduleux. Le scénario choisi imitait une notification LinkedIn indiquant à l'utilisateur qu'il a reçu un message de la platforme. L'email invitait à cliquer sur le bouton "Voir message", redirigeant la victime vers une fausse page de connexion reproduisant l'interface de connexion de LinkedIn.
Deux employés ont été ciblés dans cette simulation : l'un d'eux a ignoré le message, tandis que l'autre a non seulement cliqué sur le lien, mais a également saisi son identifiant et son mot de passe sur la page frauduleuse. Les résultats obtenus démontrent la capacité des attaquants à exploiter la confiance accordée aux plateformes professionnelles et soulignent l'importance de renforcer la formation du personnel.

Glossaire

Phishing : Technique de cyberattaques ou l'on tente de recuperer des informations personnelles.

Email template : Ce que verra l'utilisateur quand il recevra l'email

Landing page : La page que l'utilisateur aura été rediriger quand il aura cliquer sur le lien.

Sending profile : Le profile de celui qui envoyer l'email.

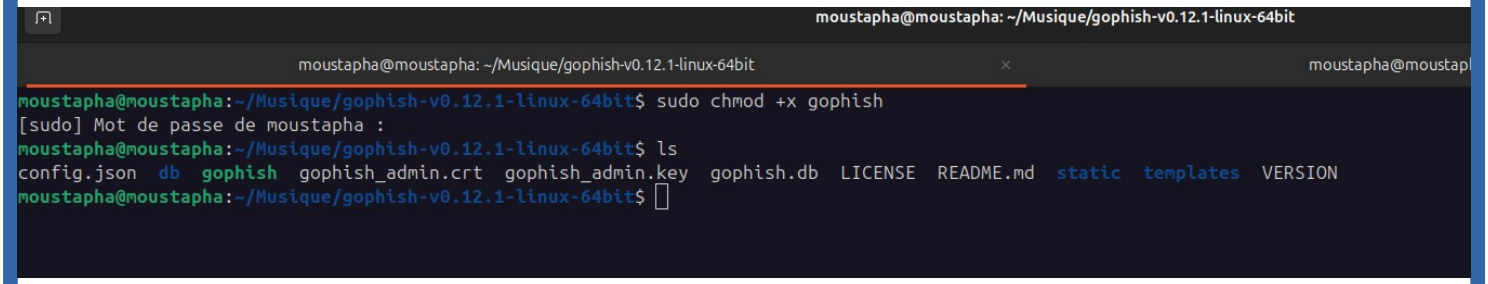
Introduction Général

La direction a souhaité évaluer le niveau de vigilance des employés face aux attaques de phishing. Le phishing demeurant l'un des vecteurs d'intrusion les plus utilisés par les attaquants, il est essentiel pour toute organisation d'en mesurer l'impact potentiel et la capacité de détection des utilisateurs. Le présent projet consiste à mettre en place une simulation d'attaque contrôlée en reproduisant un scénario réaliste, depuis la création d'un faux email frauduleux jusqu'à l'analyse du comportement des utilisateurs ciblés. Cette approche permet d'identifier les faiblesses humaines, de comprendre les mécanismes de manipulation utilisés dans ce type d'attaque et d'élaborer, à partir des résultats observés, un plan de sensibilisation destiné à réduire efficacement les risques futurs.

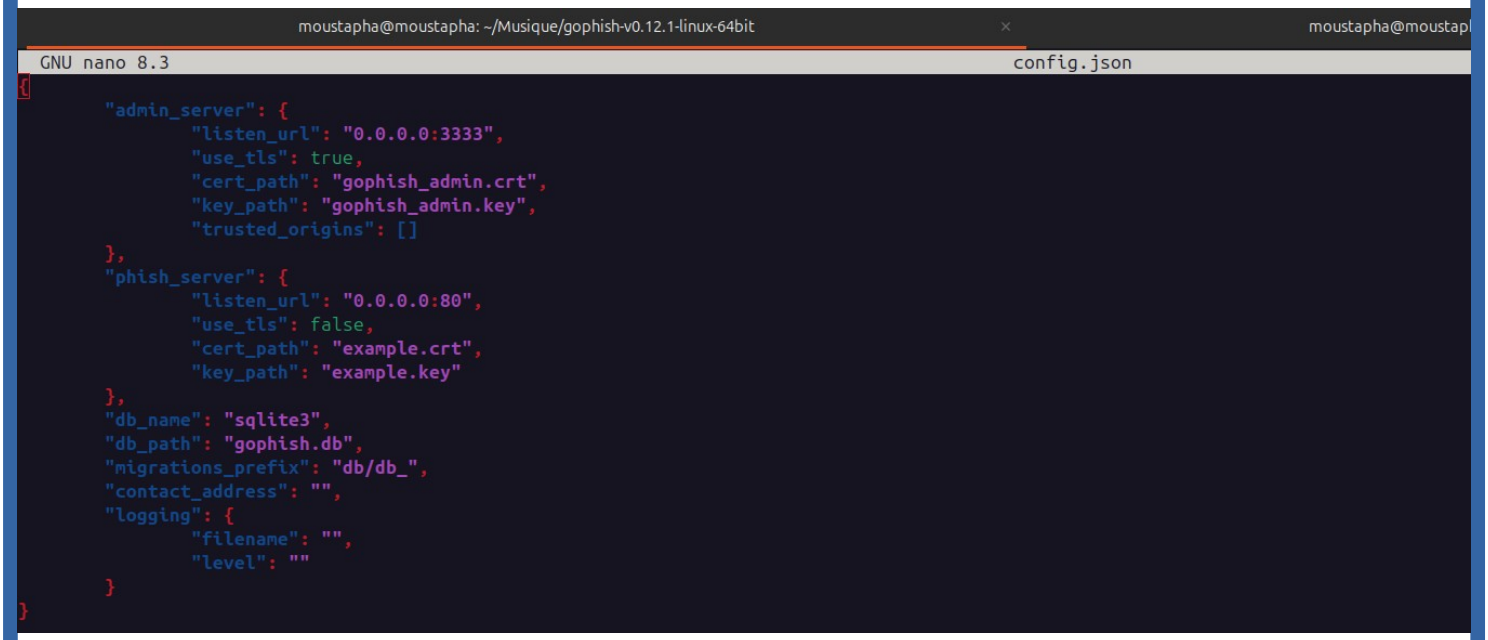
Installation de Gophish

Premièrement on télécharger le fichier zip disponible dans https://github.com/gophish/gophish/releases.
Après on dézippe le fichier

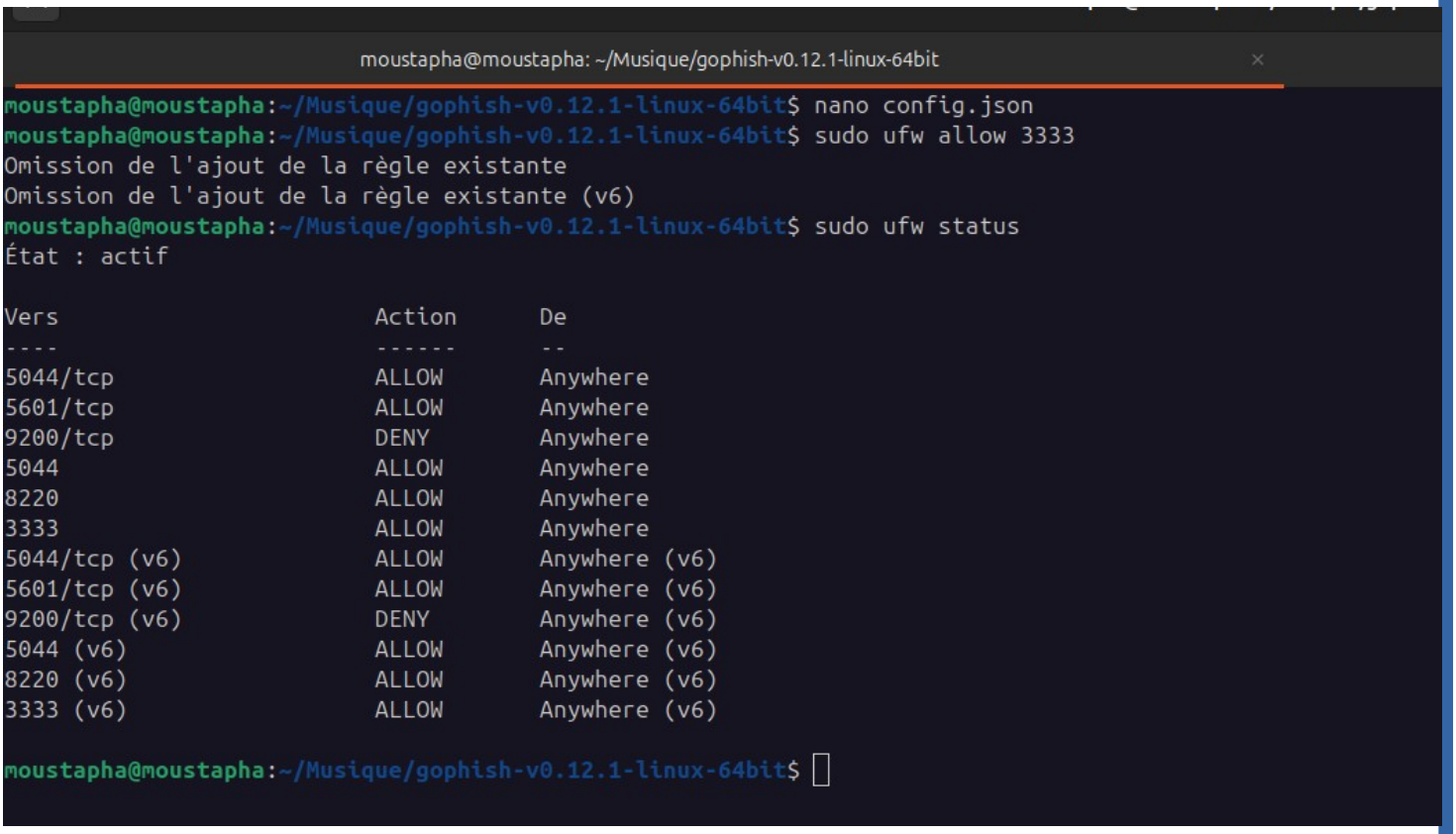
voici ce qu'on va avoir, apres avoir dézipper le fichier.



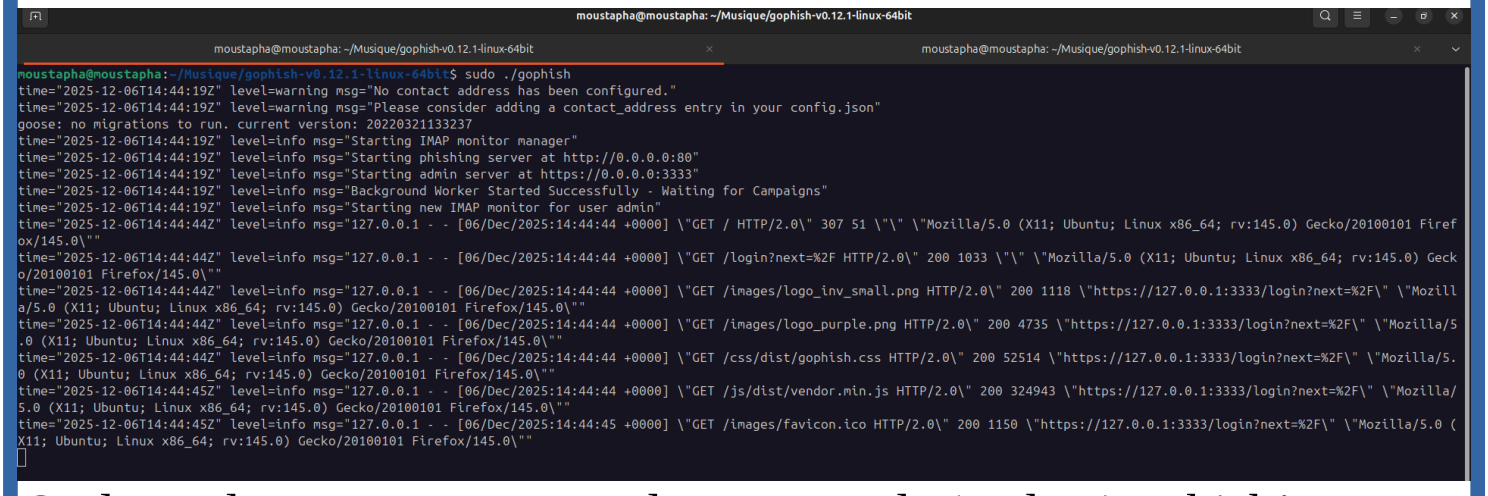
Ici on rend executable le programme 'gophish' avec la commande 'chmod +x gophish'



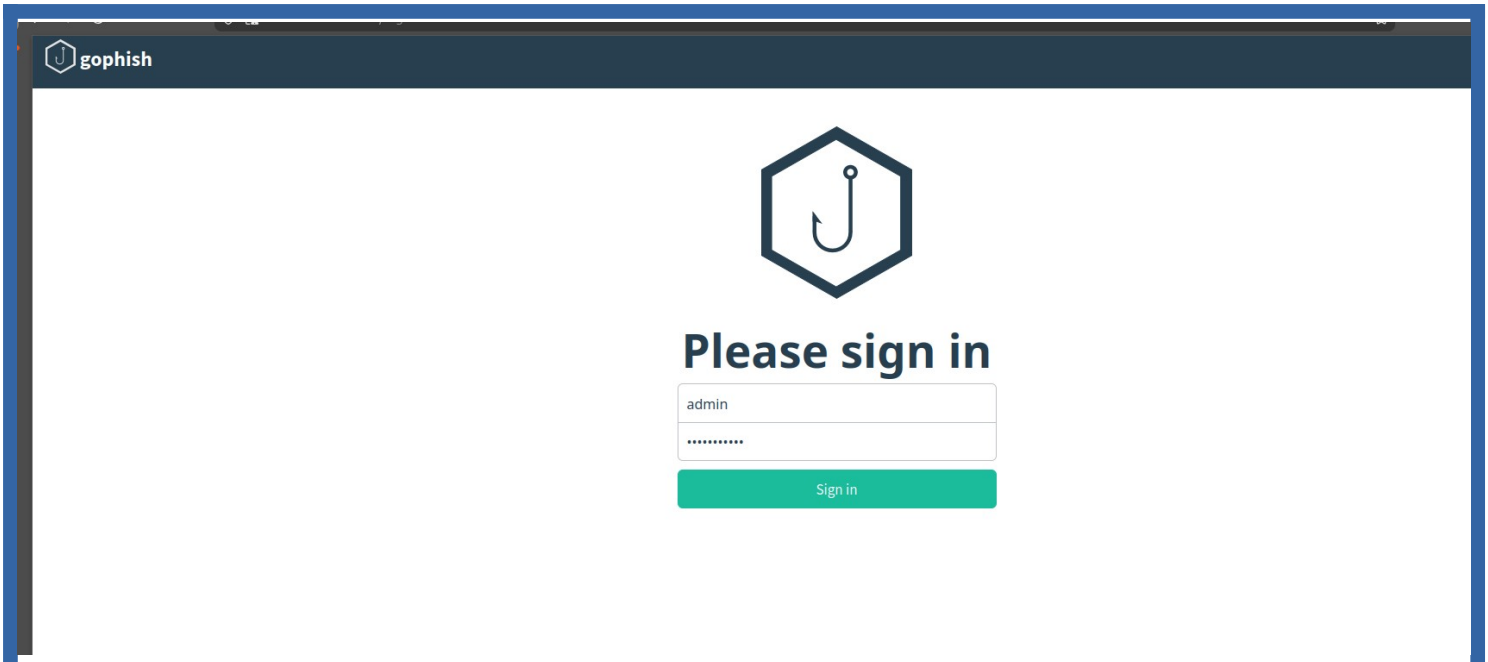
Dans notre fichier config.json, on modifie 127.0.0.1 par 0.0.0.0, pour pouvoir acceder à gophish depuis l'extérieur.



Ici on autorise le port 3333 avec la commande 'sudo ufw allow 3333'.

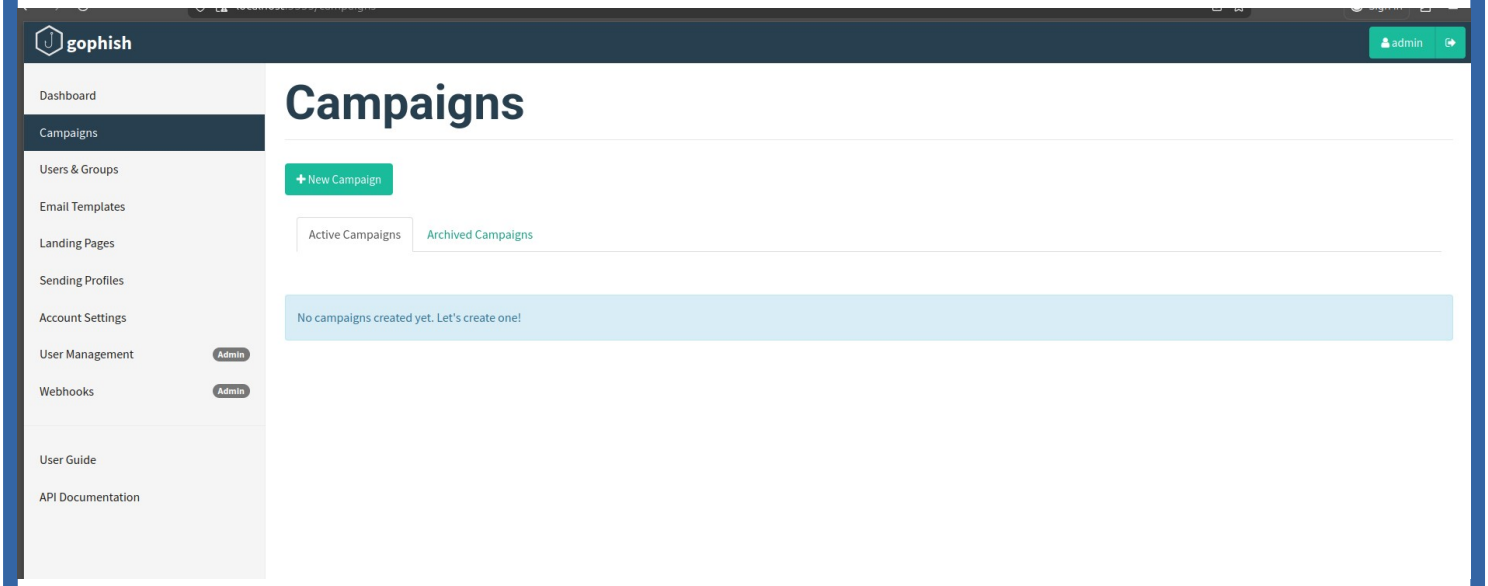


On lance le programme avec la commande 'sudo ./gophish'
NB : Lors du premier lancement, un mot de passe vous sera donné afin de vous connecter avec admin/votre_mot_de_passe

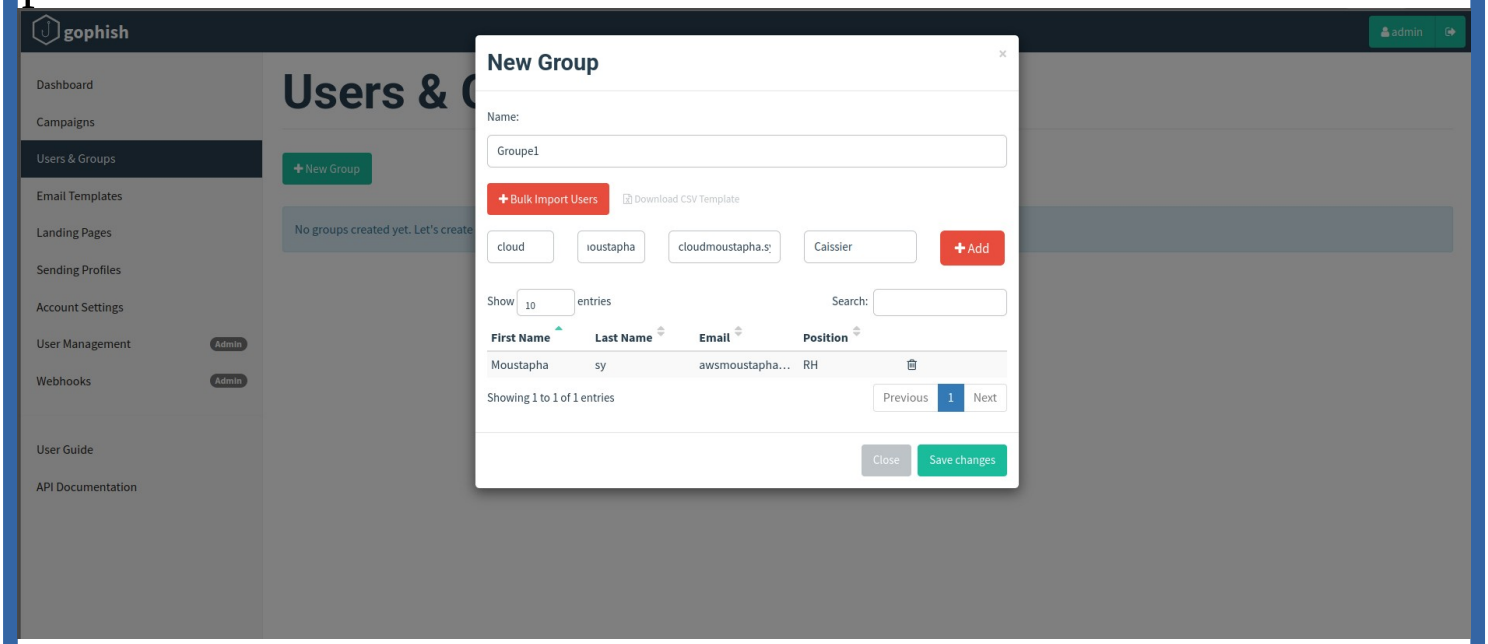


Une fois lancé le programme gophish, on se rend dans le navigateur et saisi l’adresse https://localhost:3333 , puis se connecter avec notre login et mot de passe (qui sera changer apres)

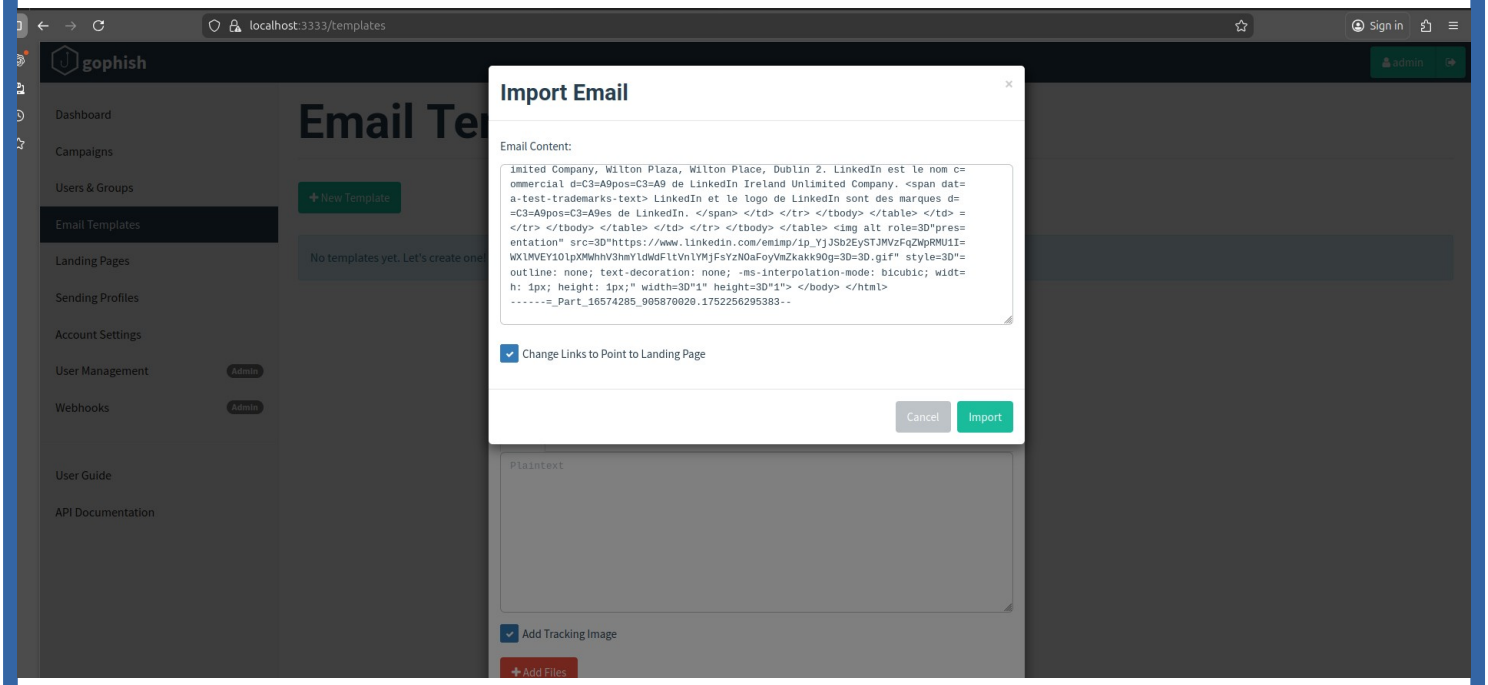
Mise en place de la campagne



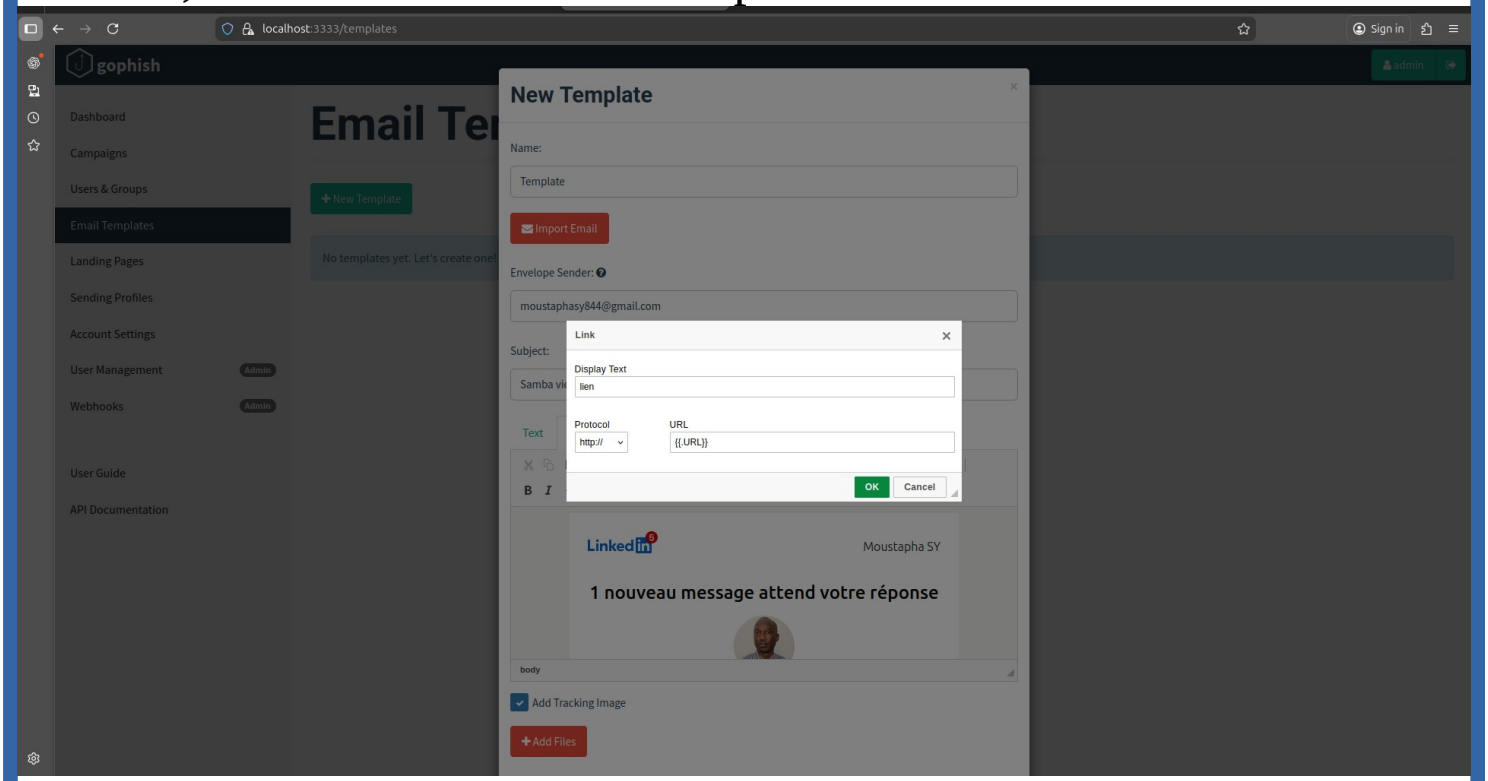
Avant de créer la campagne, on doit dabord créer un groupe d'utilisateurs , un email template, un landing page et un sending profile.



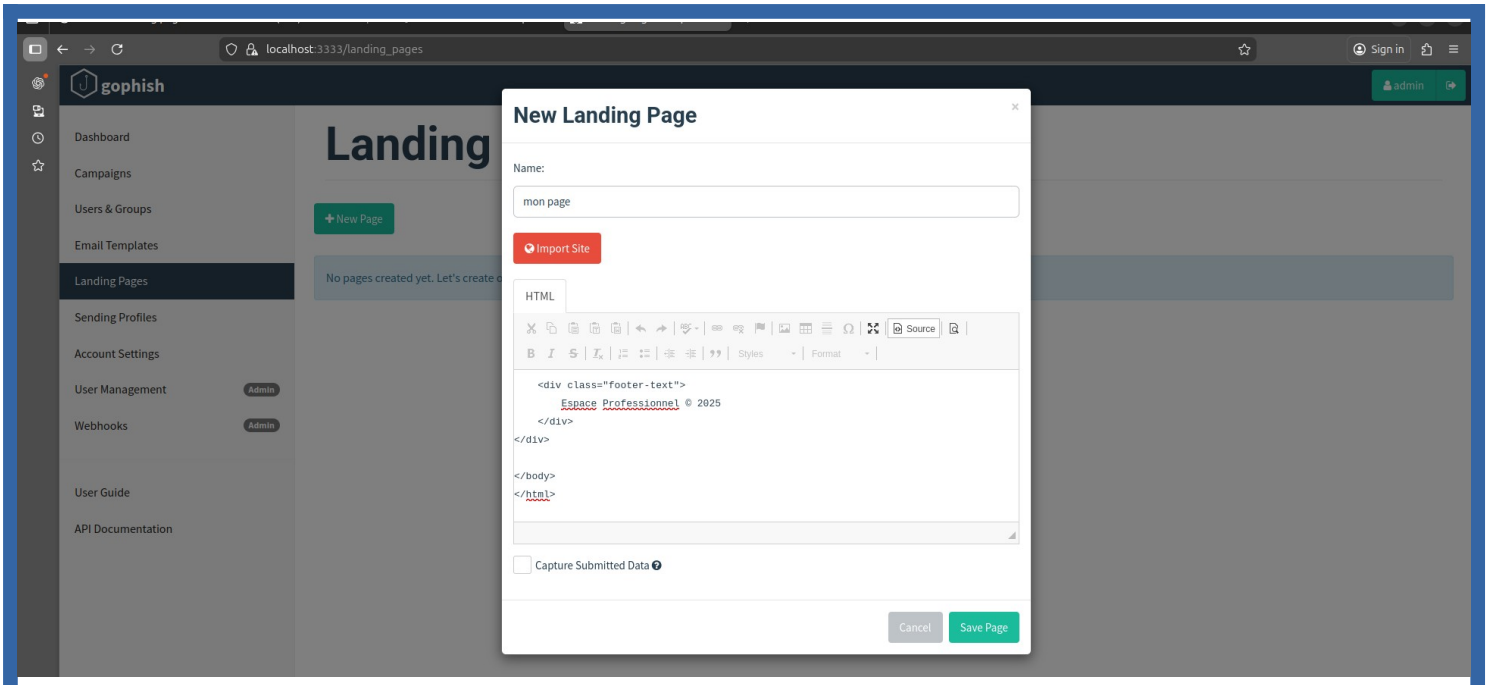
Ici nous avons créer un groupe nommé 'groupe1' avec deux utilisateurs



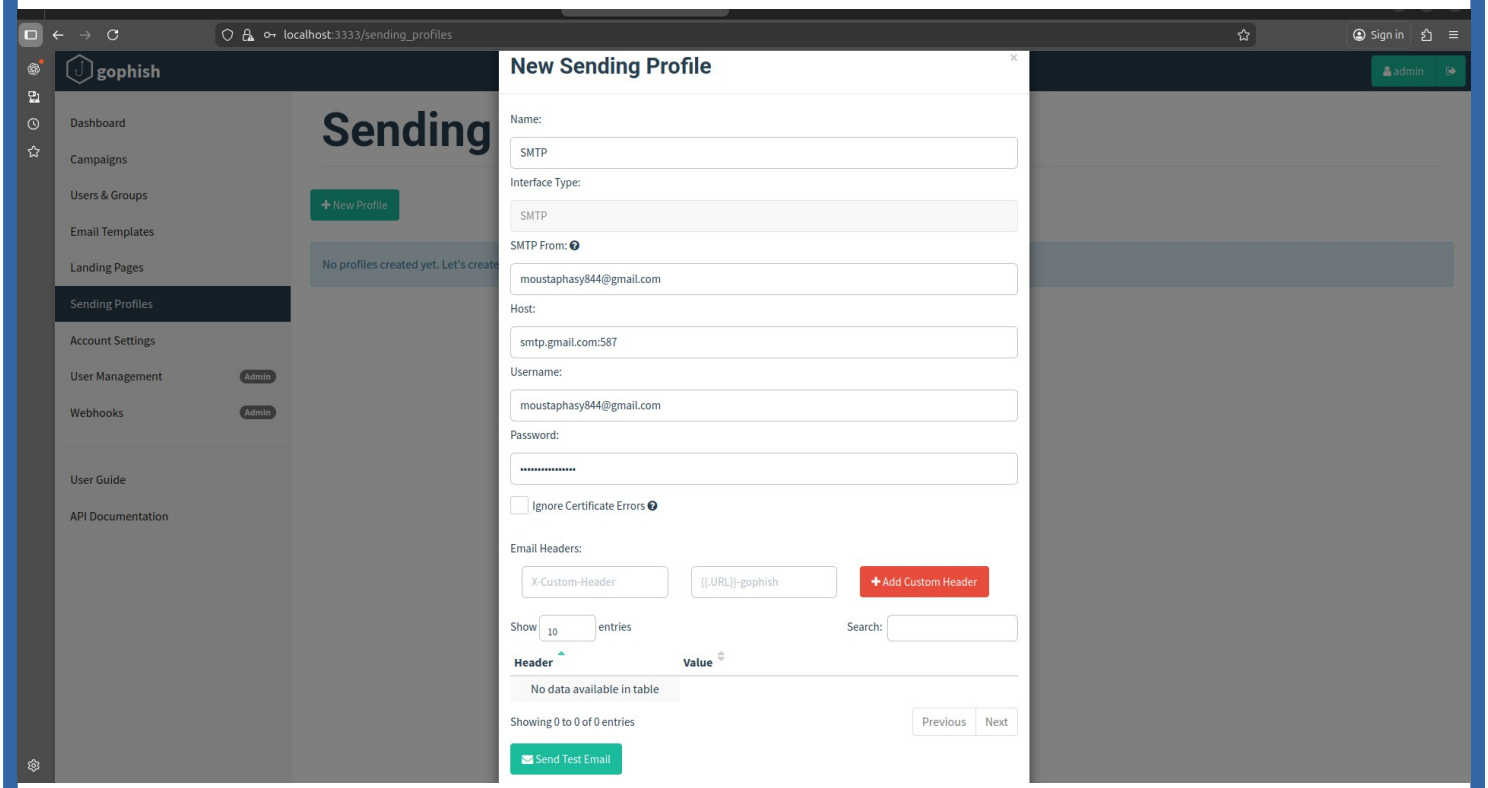
Ensuite, on a créer une email template.



Toujours dans l’email template , on ajoute l’url en mettant {{.URL}} (cette url sera spécifier lors de la création de la campagne)

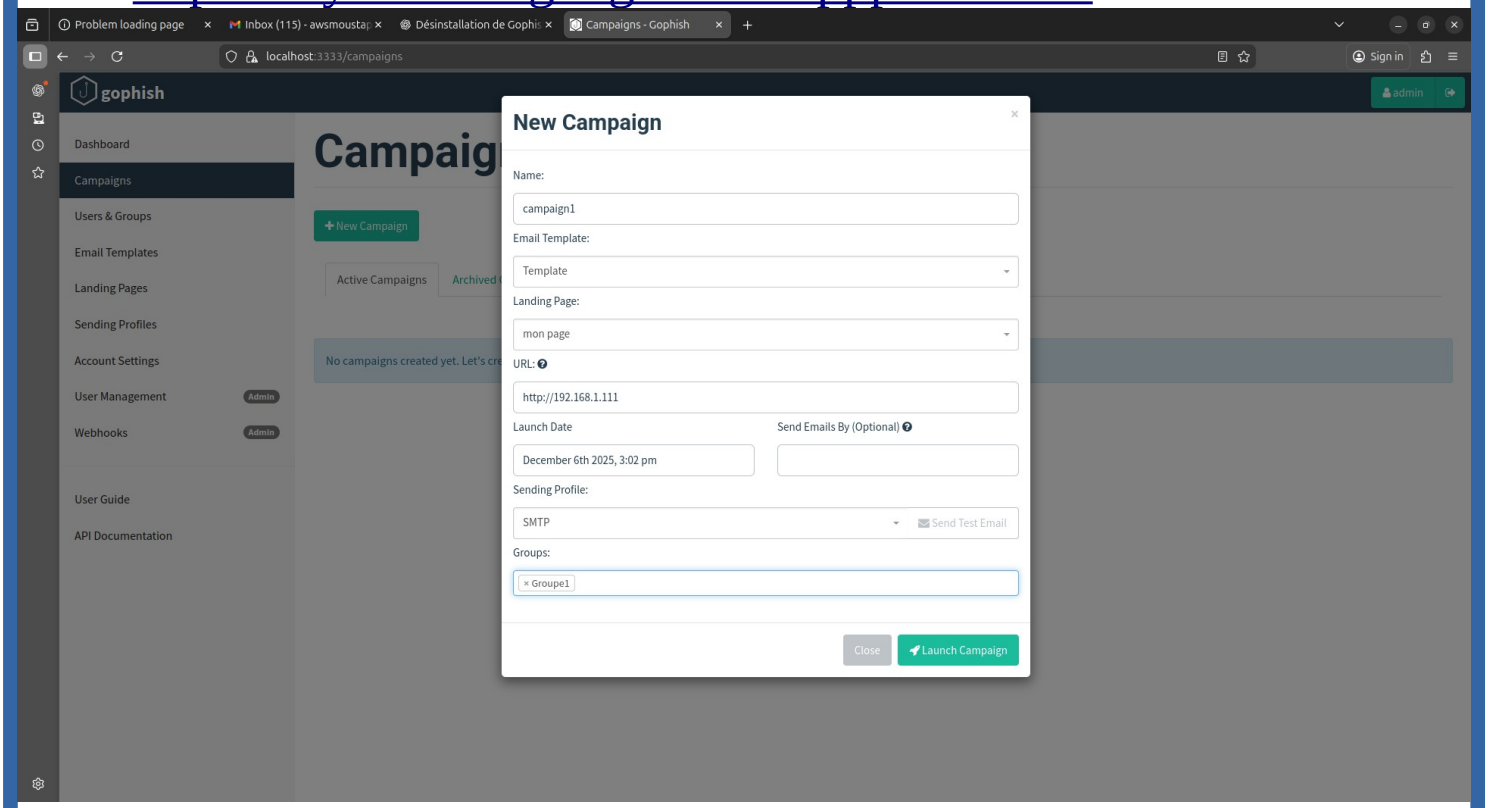


Apres l’email template , ici on va créer notre landing page.
Le landing page cest ce que verra l’utilisateur après avoir cliquer sur le lien, dans notre cas c’est une page de connexions.

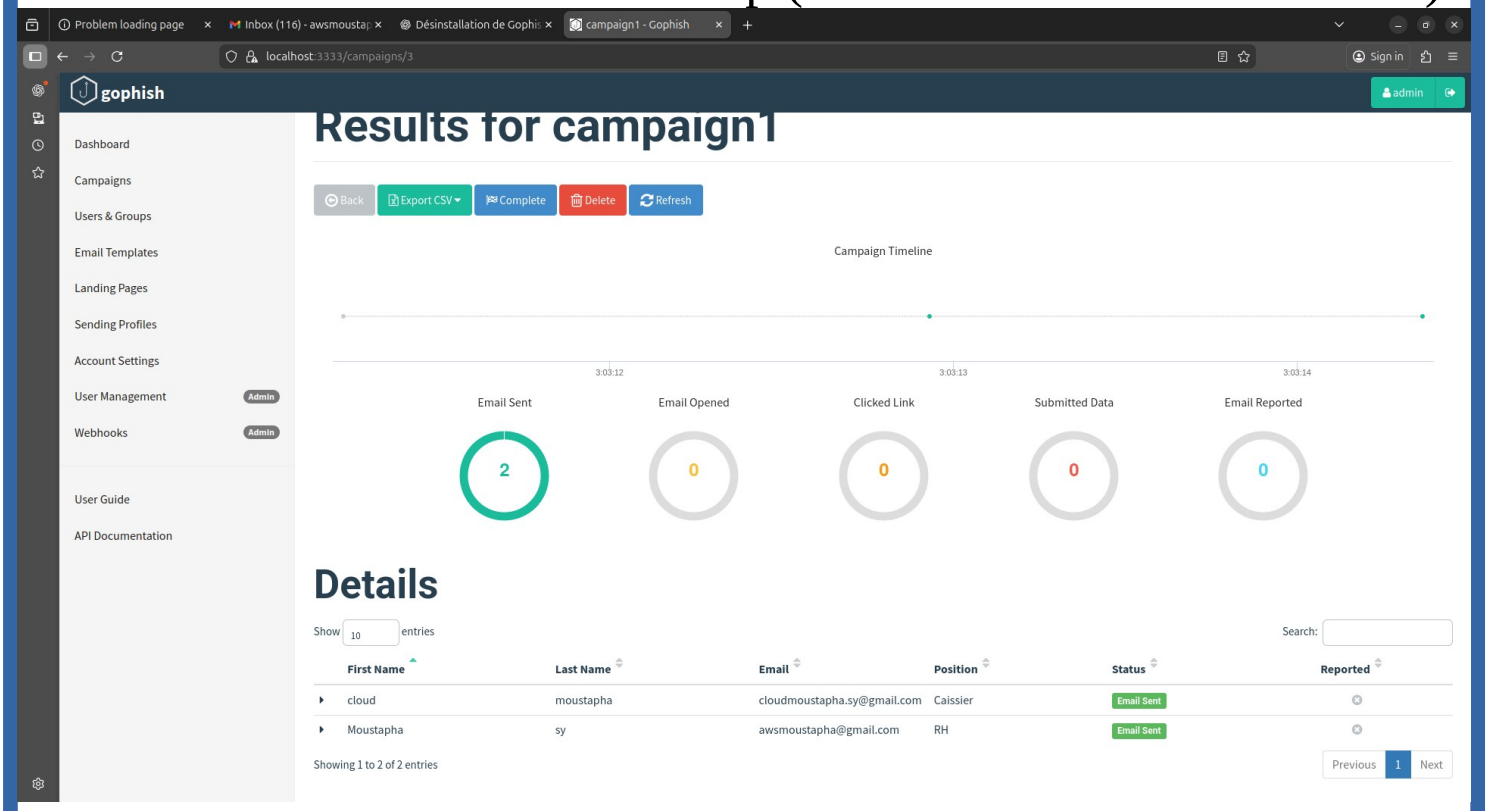


Ici en crée le sending profile, qui est le profile de celui qui va envoyer le message.

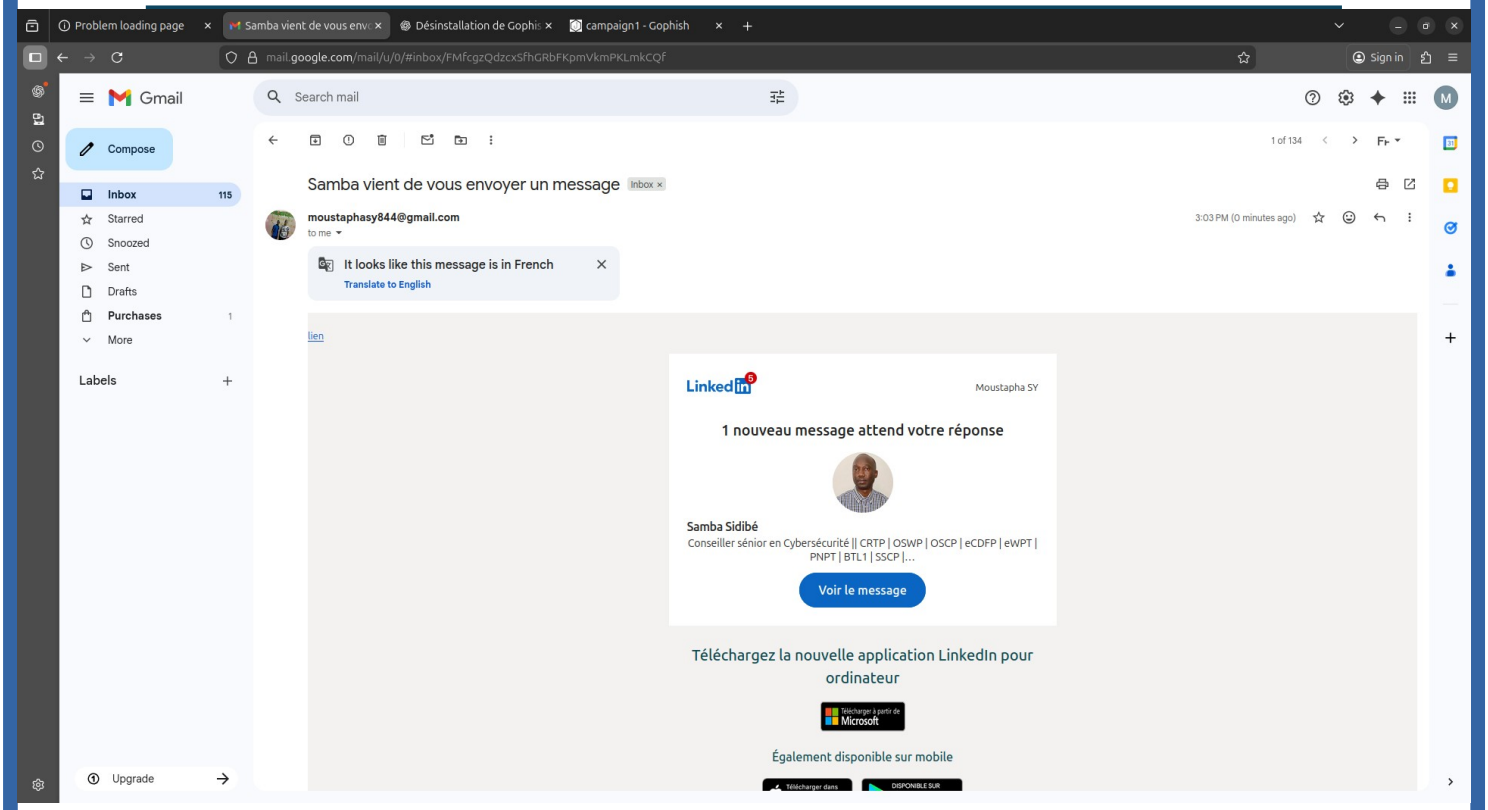
Pour le username, il faut mettre l’adresse email de l’expéditeur, et le mot de passe , cest le mot de passe application qui sera générer dans https://myaccount.google.com/apppasswords .



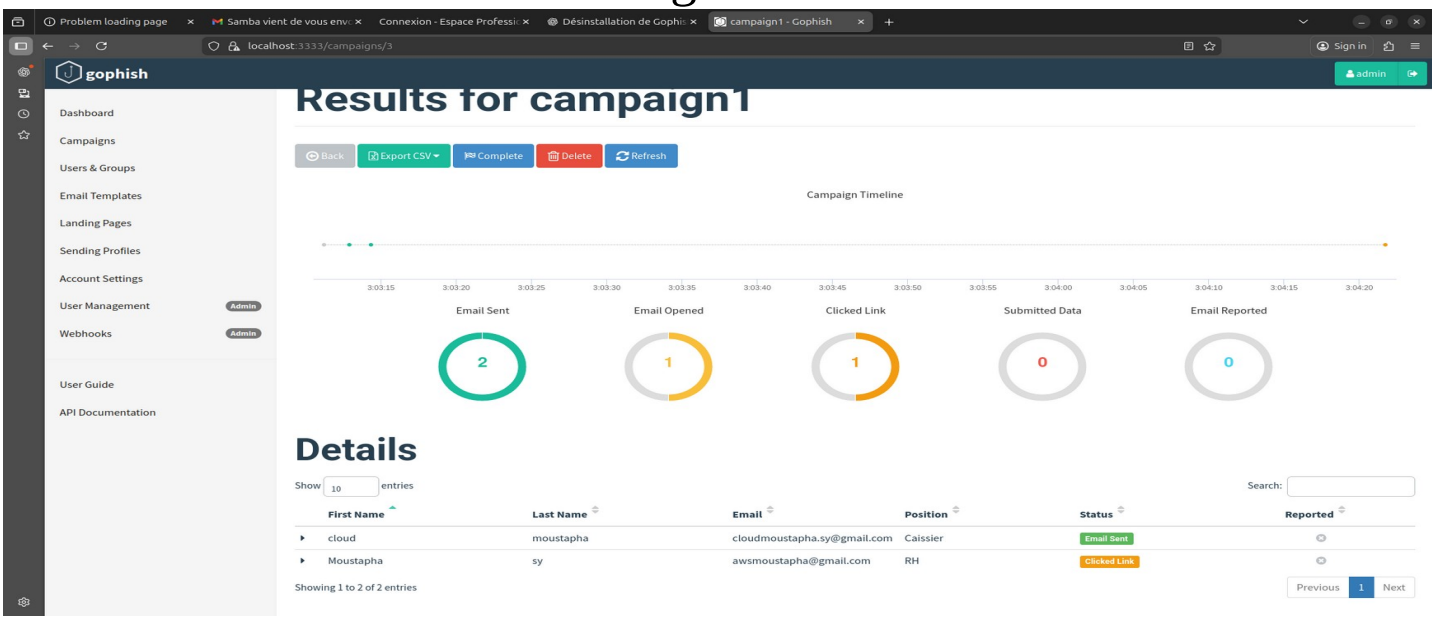
Apres tout ca faite , on peut maintenant créer la campagne , en mettant comme url notre adresse ip (ou nom de domaine si existe)



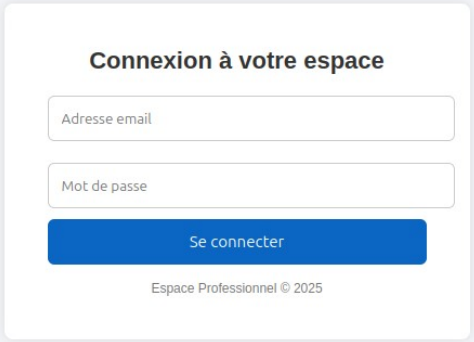
Collecte des clics et réponses des utilisateurs



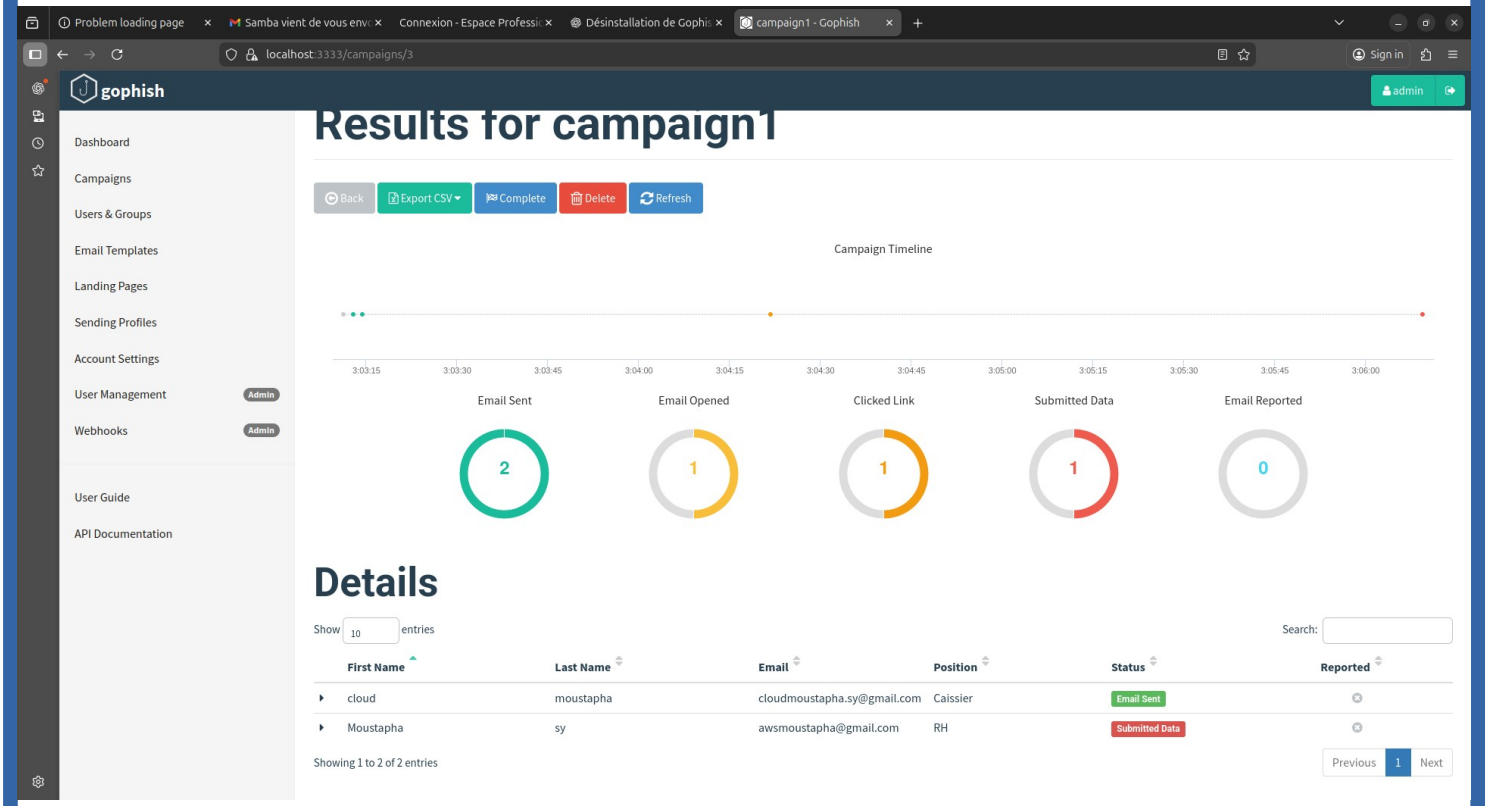
voici l’email qui a été envoyer(le danger se trouve quand l’utilisateur clic sur ‘voir message’



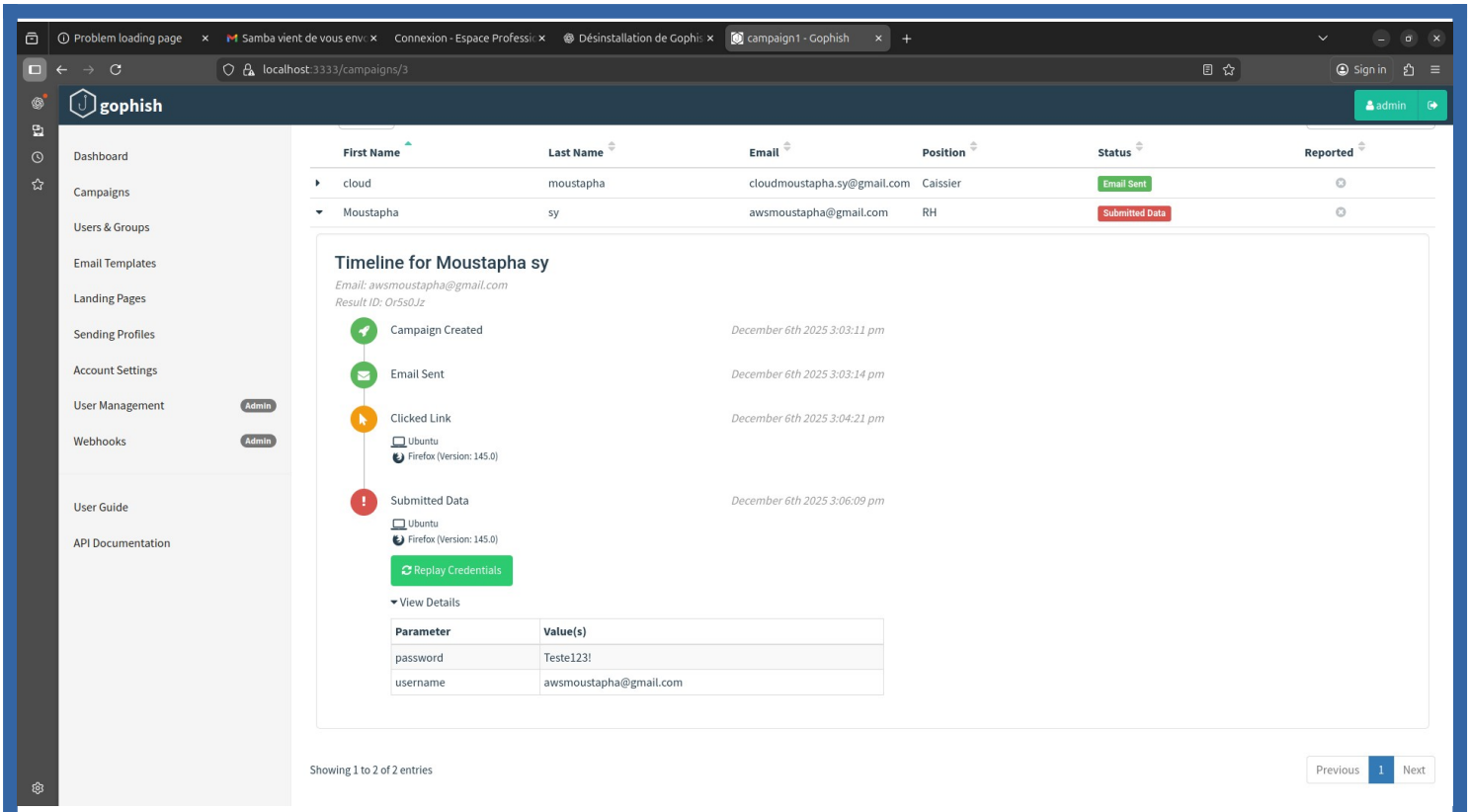
Dans le resultat de la campagne, on peut voir que l’email a été envoyer par deux utilisateurs et que l’une a cliquer sur le lien.



Une fois cliquer l’utilisateur verra ceci



D’apres les résultat, l’utilisateur a renseigner ces informations



Et on peut voir les informations de l’utilisateur comme son username et mot de passe.

Plan de sensibilisation

Suite à la campagne de phishing réaliser via Gophish, il est essentiel en premier lieu d’informer le personnel sur les méthodes utilisées par les attaquants, les conséquences possibles d’un mail frauduleux. Une communication claire, accompagnée de fiche simple et de message interne, permet de rappeler régulièrement les réflexes essentiels. Il est également nécessaire de mettre en place un canal de signalement des emails suspects afin d’encourager les utilisateurs à alerter rapidement l’équipe informatique. Aussi les campagnes de phishing doivent être faite de façons régulières. Enfin, des mesures de techniques anti-phishing devrait être mis en place afin d’ajouter une couche supplémentaire de sécurité.

Conclusion

Cette simulation de phishing a permis de mettre en évidence la vulnérabilité persistante du personnel face aux attaques d'ingénierie sociale. Malgré le faible nombre de personnes ciblées, le fait qu'un employé ait cliqué sur le lien frauduleux et renseigné ses identifiants démontre qu'un attaquant aurait pu obtenir un accès critique en conditions réelles. Ce test confirme que la sensibilisation doit rester une priorité stratégique pour une organisation. Les résultats obtenus servent ainsi de base à la mise en place d'un programme de formation adapté, visant à renforcer les réflexes de vérification, améliorer la détection des messages suspects et instaurer une culture de vigilance durable. En poursuivant régulièrement ce type de campagne et en sensibilisant le personnel aux bonnes pratiques, une entreprise pourra significativement réduire les risques liés aux tentatives de phishing futures.