BTS SIO SISR

Situation professionnelle numéro 6

Mise en place et configuration d'une campagne de phishing

C'est lors de cette situation que je vais essayer de répondre à la problématique.

BTS SIO SISR CFA INSTA 75005

Léo LE CORRE

Plan de situation :

La demande

KLLT Bank souhaite déployer une campagne interne de phishing afin d'évaluer la vigilance de ses employés et renforcer sa stratégie de sensibilisation. En tant que banque, elle est fortement exposée aux attaques par ingénierie sociale, souvent utilisées pour dérober des identifiants ou obtenir un accès initial au réseau. L'objectif est donc de mettre en place, via l'outil GoPhish, une simulation réaliste permettant de mesurer les comportements à risque (ouverture, clic, saisie de données) et d'identifier les besoins en formation. Cette campagne doit fournir à l'entreprise une vision claire du niveau de maturité de ses collaborateurs face aux mails malveillants et permettre d'améliorer ses pratiques de sécurité.

C'est quoi le phishing ?

Le phishing ou hameçonnage est une technique frauduleuse incitant la victime à communiquer ses données personnelles. L'attaquant se faisant passer pour une entité ou un proche.

88 % des violations de la cybersécurité sont causées par des erreurs humaines

94 % des logiciels malveillants sont transmis par e-mail

En 2024, le hameçonnage classique avec un lien malveillant représente 56 % des attaques de phishing.

Exemples :

- Votre compte Microsoft sera suspendu. Veuillez vérifier votre identité avant minuit.
- Activité suspecte détectée sur votre compte bancaire. Connectez-vous pour confirmer les opérations.

C’est quoi GoPhish ?

Gophish est une plateforme open-source conçue pour aider les organisations à simuler des attaques de phishing et renforcer leur sensibilisation à la cybersécurité. Présent nativement sur certaines distributions Linux (spécifiques à la sécurité informatique comme Kali Linux et BlackArch Linux), c’est la solution open source optimale.

Il permet également d’effectuer un suivi des résultats des campagnes au fur et à mesure du temps pour pouvoir noter l’évolution, ainsi qu’une personnalisation infinie permettant de cibler au mieux certains métiers/services.

Enfin, étant open source et auto-hébergeable, il garantit un contrôle total sur les données collectées tout en permettant une traçabilité complète des actions, ce qui facilite l’audit interne et l’amélioration continue de la sensibilisation des équipes.

Pourquoi GoPhish ?

GoPhish a été retenu car il s’agit d’une solution open-source complète, simple à déployer et entièrement personnalisable, ce qui en fait un outil idéal pour mener une campagne de phishing interne. Contrairement à des solutions payantes comme KnowBe4 ou PhishInsight, qui offrent une interface très aboutie mais nécessitent un abonnement coûteux, GoPhish permet de réaliser des tests professionnels sans frais, tout en gardant un contrôle total sur les scénarios, les modèles de mails et les résultats. Par rapport à King Phisher, plus complexe à configurer et nécessitant une infrastructure plus lourde, GoPhish se distingue par sa rapidité de mise en place et son interface intuitive. Enfin, contrairement à des solutions plus simples comme Lucy Community Edition, qui peut manquer de flexibilité et de fonctions avancées, GoPhish propose un bon équilibre entre facilité d’utilisation et puissance.

Au final, GoPhish offre à KLLT Bank la meilleure combinaison : gratuit, flexible, rapide à déployer et suffisamment complet pour réaliser des simulations réalistes, analyser les comportements et produire des rapports utiles à l’amélioration de la sensibilisation interne. C’est donc la solution la plus adaptée pour une campagne efficace, maîtrisée et économiquement rentable.

Pourquoi mettre en place une campagne de phishing ?

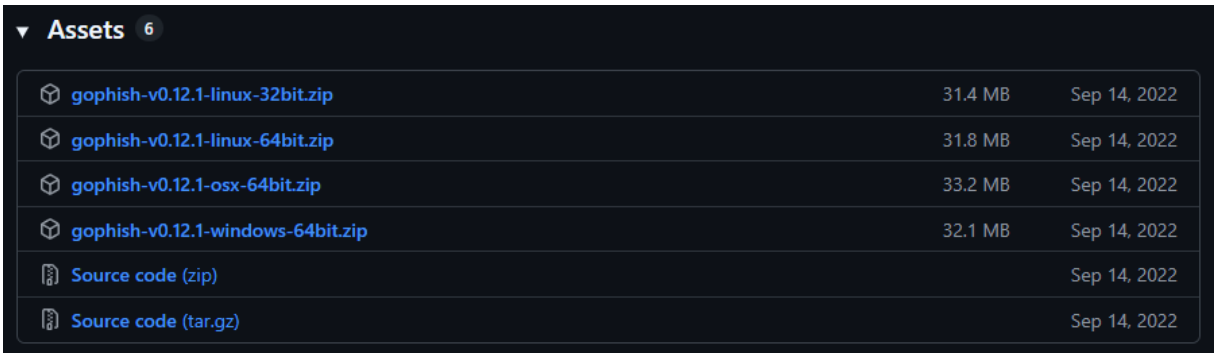
La mise en place de campagnes de phishing est essentielle pour KLLT Bank, car elles permettent d'identifier et de corriger les comportements pouvant conduire à des incidents graves. Un simple clic sur un mail malveillant peut permettre à un attaquant d'obtenir un mot de passe faible ou réutilisé, facilitant ensuite la propagation latérale ou l'élévation de privilèges dans le réseau de l'entreprise. Ces erreurs humaines peuvent également entraîner des fuites de données, une exfiltration d'informations sensibles, ou encore la compromission du principe CID (Confidentialité, Intégrité, Disponibilité), qui est au cœur des exigences de sécurité d'un établissement bancaire.

Au-delà des aspects techniques, une attaque réussie peut avoir un impact direct sur la réputation de la banque : perte de confiance des clients, médiatisation négative et atteinte durable à l'image. Les conséquences peuvent aussi être juridiques, notamment en cas de violation du RGPD, de sanction de la CNIL ou de non-protection suffisante des données personnelles. Les campagnes de phishing permettent donc d'anticiper ces risques, de mesurer le niveau de vigilance des employés et d'améliorer la sensibilisation globale afin de réduire la probabilité d'un incident ou d'un accident majeur.

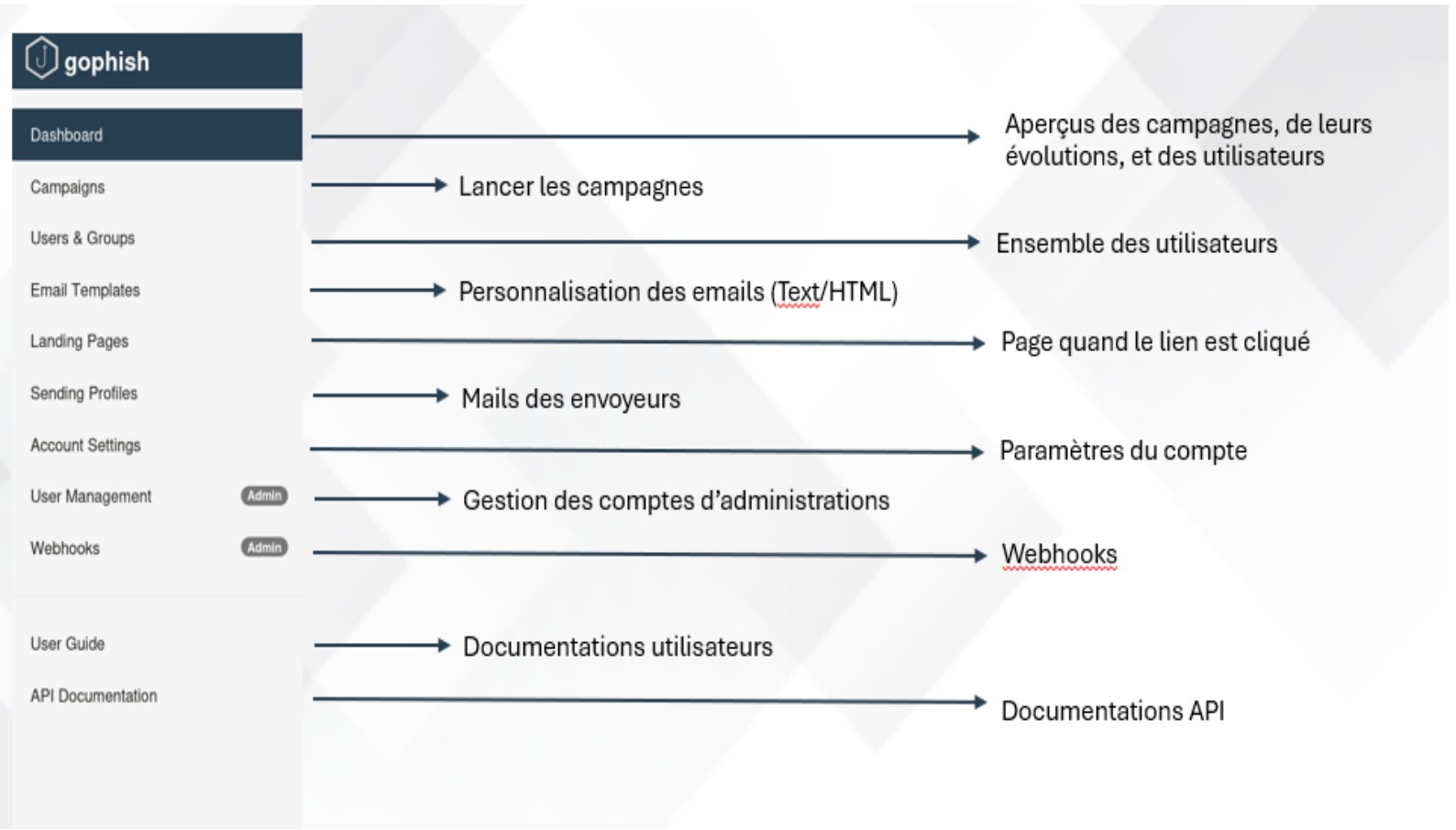
Installation de l'outil

GoPhish s'installe très simplement. Sous Windows, il suffit de télécharger l'archive ZIP depuis le site officiel, de l'extraire puis de lancer le fichier gophish.exe. L'outil démarre immédiatement et l'interface d'administration est accessible via le navigateur à l'adresse https://127.0.0.1:3333.
Sous Linux, l'installation consiste à télécharger l'archive, la décompresser, donner les droits d'exécution au fichier gophish puis le lancer. Une fois démarré,

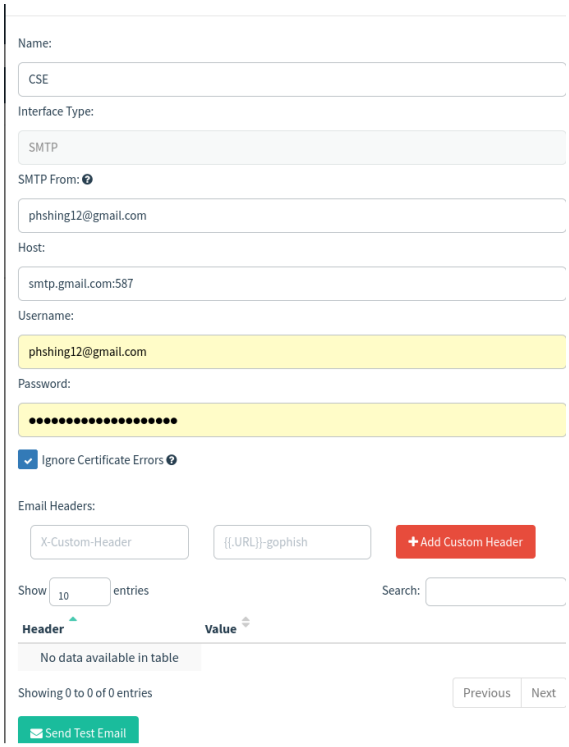
l'accès se fait également via https://<IP>:3333. Dans les deux cas, aucune installation complexe n'est nécessaire, GoPhish fonctionne dès son exécution.



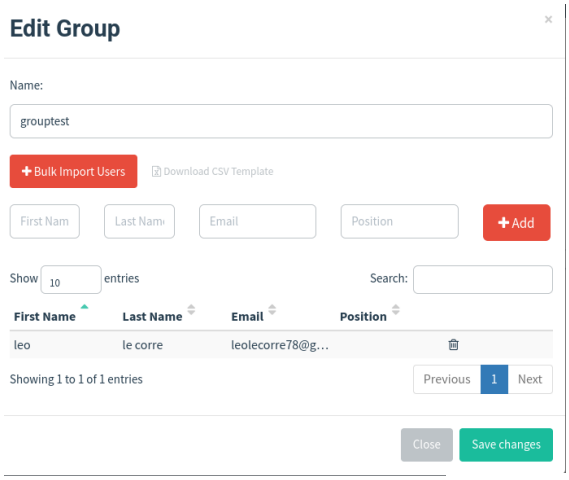
Vue d'ensemble de l'outil



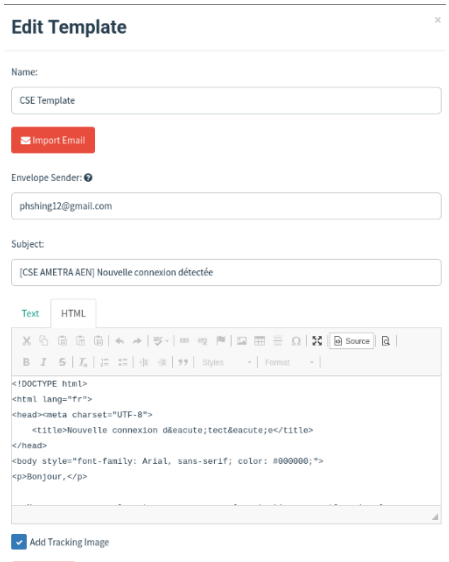
Configuration de l'outil



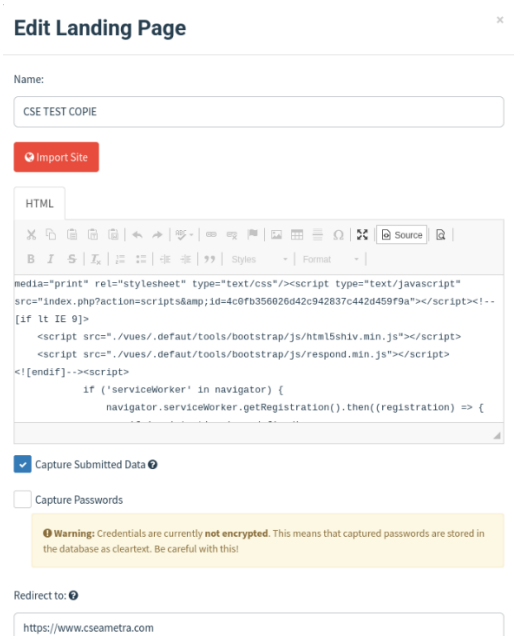
Il faut commencer par lier l'e-mail de l'envoyeur à Gophish, en mettant un nom, le protocole, l'adresse e-mail, l'host, le username, le mot de passe, et cocher « ignorer les erreurs de certificats ».



Puis on va définir la liste des cibles



On va préparer le mail avec les liens dedans, on met le nom de l'e-mail, l'envoyeur, l'objet, et le contenu du mail en HTML

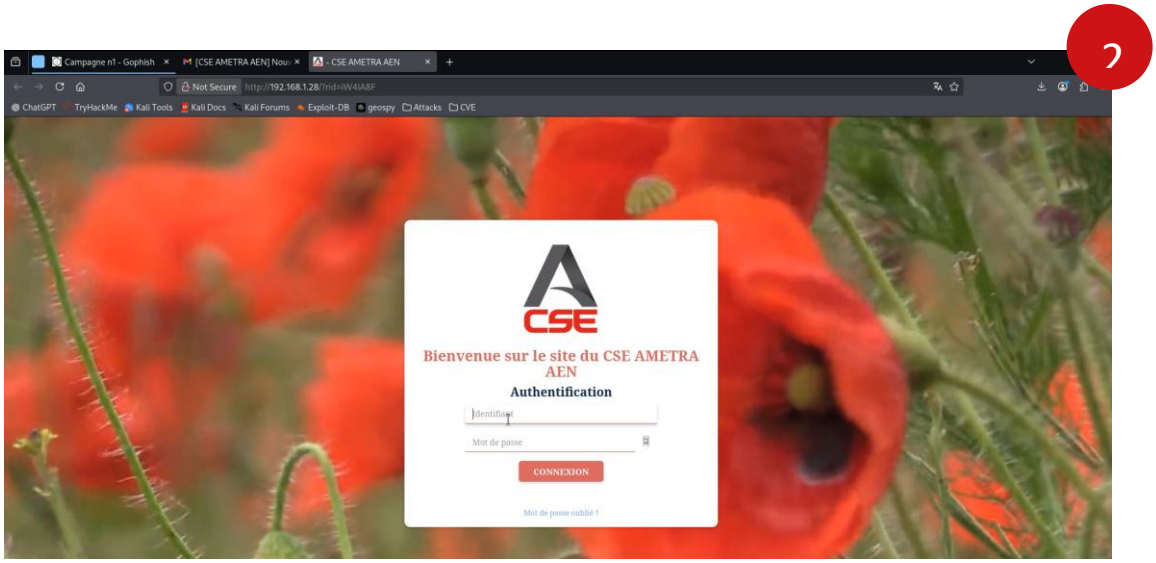


Enfin, on fait la page sur laquelle les utilisateurs vont tomber quand ils cliqueront sur le lien qui est à l'intérieur du mail, en lui donnant un nom, en mettant le code de la page en html/css, et en cliquant sur « Capture Submitted Data » ainsi que redirect, en mettant le lien sur lequel les utilisateurs tomberont quand ils auront cliqué sur connexion.

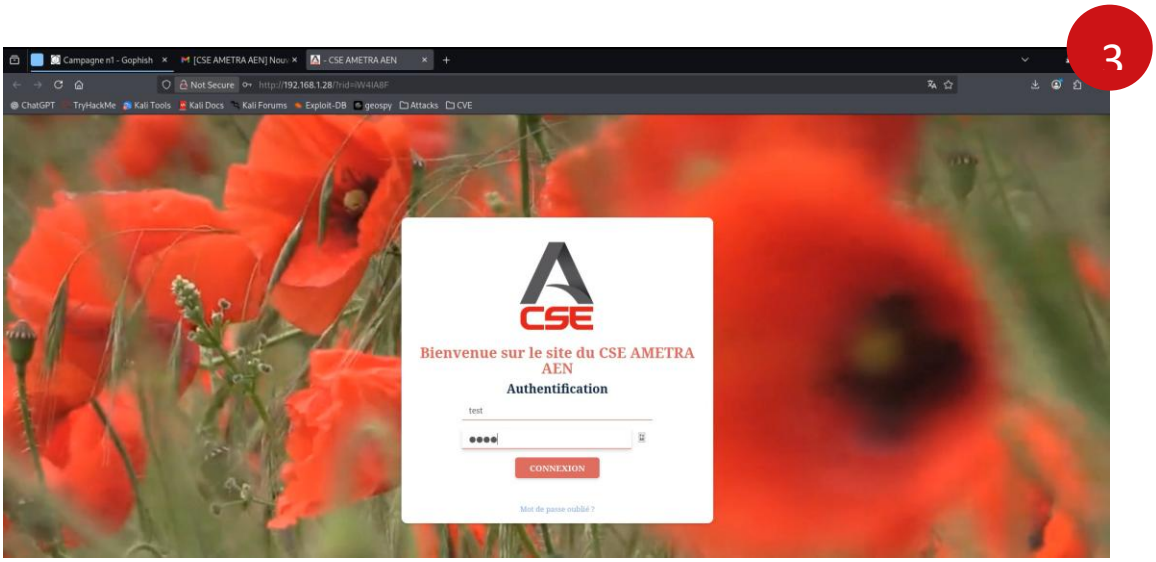
Enfin, on peut lancer la campagne.

Test du point de vue de l'utilisateur

En premier lieu, l'utilisateur vas recevoir le mail.

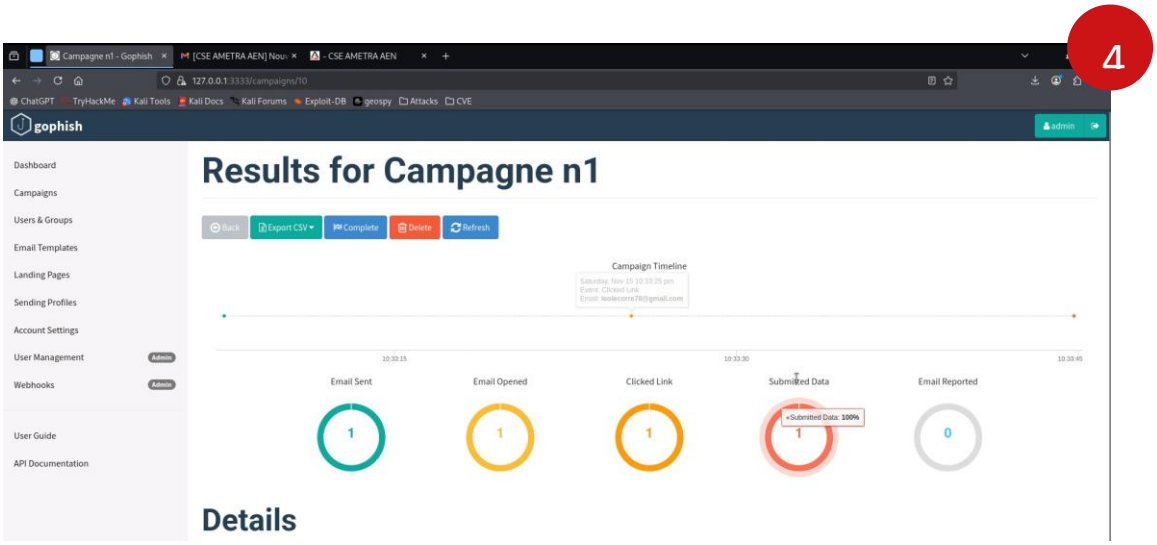


Puis, l'utilisateur vas cliquer sur le lien.



L'utilisateur vas rentrer ses identifiants puis cliquer sur « Connexion ».

Résultat



Enfin, on peut voir dans le Dashboard qu'un email à été envoyé, ouvert, qu'un lien à été cliqué et des données ont été envoyées.

Résumé

La démonstration de la campagne de phishing avec GoPhish a permis de présenter l'ensemble du processus, de l'installation à la configuration, en passant par l'envoi simulé d'e-mails et la capture de données fictives. Même si aucun utilisateur réel n'a interagi avec la campagne, cette simulation a permis de comprendre le fonctionnement de l'outil et de visualiser le suivi des résultats via le tableau de bord.

Ce projet montre que GoPhish est une solution simple à déployer, flexible et adaptée pour réaliser des campagnes de sensibilisation au phishing. Il offre à l'entreprise la possibilité d'évaluer le niveau de vigilance de ses collaborateurs, d'identifier les comportements à risque et de préparer des actions de formation ciblées.

En résumé, cette démonstration constitue une base solide pour la mise en place de campagnes et contribue à renforcer la sensibilisation à la sécurité au sein de KLLT Bank.