Ip : 85.69.173.98, login : user, Password : walouwlouuwlaou

Projet de Sensibilisation à la Cybersécurité

Simulation de Phishing Éducative

Introduction

Dans le cadre de mes études en cybersécurité, j'ai réalisé un projet de simulation de phishing à but pédagogique. Cette expérience avait pour objectif de comprendre les mécanismes de cette cybermenace répandue et de sensibiliser à l'importance des bonnes pratiques de sécurité numérique.

Note: Ce projet a été réalisé uniquement dans un cadre éducatif contrôlé avec l'accord explicite des parties impliquées.

Objectifs du Projet

- Démontrer les techniques employées dans les campagnes de phishing
- Mettre en œuvre une infrastructure complète de simulation
- Analyser l'efficacité des différentes approches
- Évaluer la sensibilisation des utilisateurs aux risques

Méthodologie

La simulation a été organisée en suivant une méthodologie structurée en plusieurs phases:

1. Préparation de l'Infrastructure

Pour cette simulation, j'ai utilisé **Zphisher**, un outil open source dédié à la formation et à la sensibilisation en cybersécurité:

```
git clone --depth=1 https://github.com/htr-tech/zphisher.git
cd zphisher
bash zphisher.sh
```

2. Configuration de la Simulation

La campagne a été configurée pour simuler une connexion GitHub, un service largement utilisé par les développeurs:

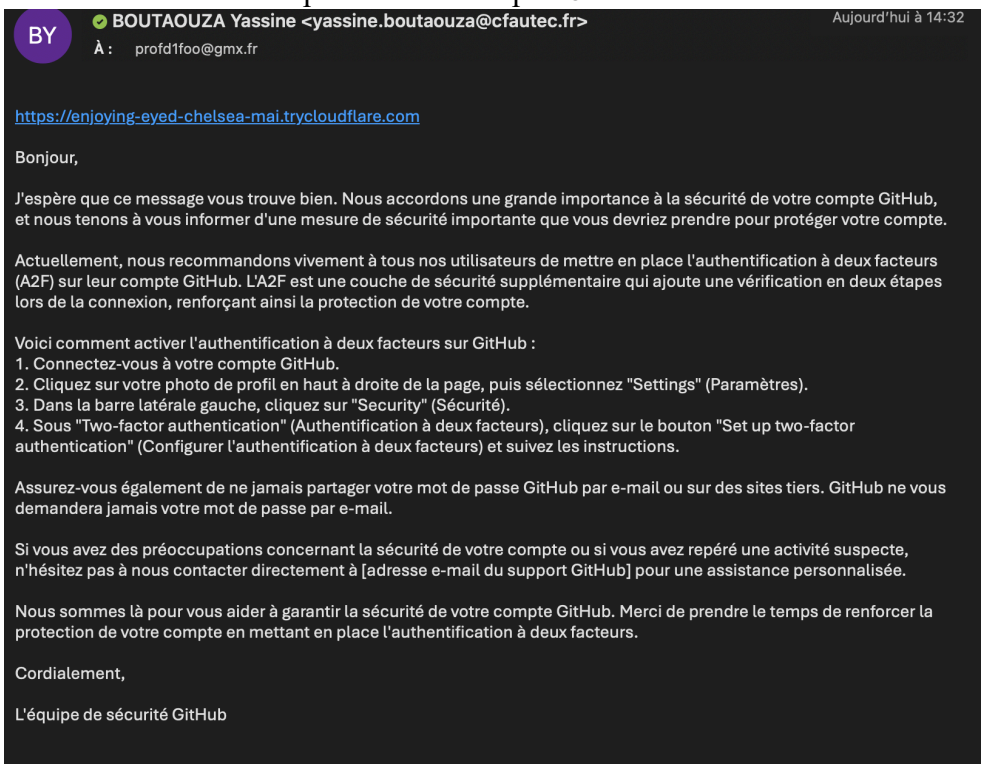
- Sélection du template GitHub parmi les options disponibles
- Configuration du serveur web sur un port dédié
- Déploiement via Cloudflare pour obtenir une URL temporaire

Ip : 85.69.173.98, login : user, Password : walouwlouuwlaou

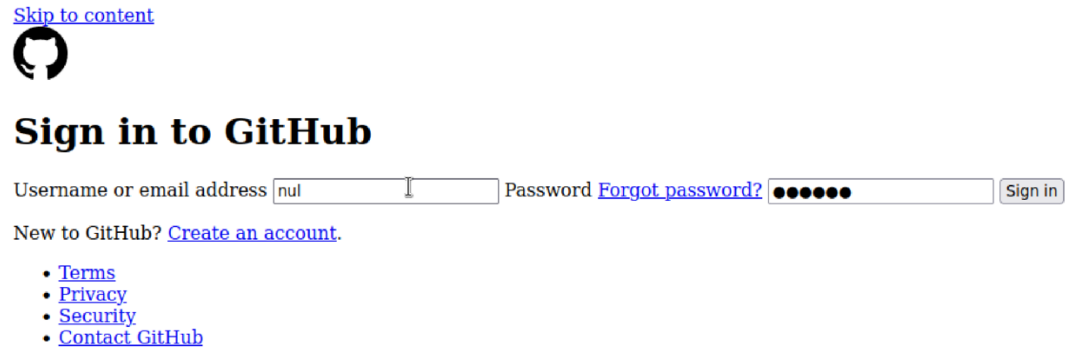
L'URL générée pour cette simulation était: `https://example-simulation-url.trycloudflare.com`

3. Élaboration du Message

J'ai créé un message ciblé simulant une notification GitHub demandant une connexion pour vérifier une activité suspecte sur le compte: c

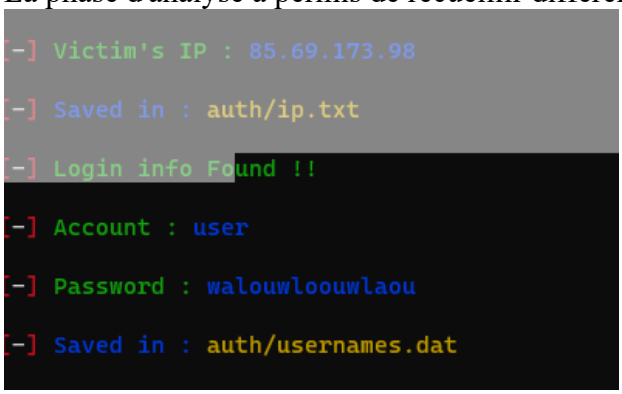


Ip : 85.69.173.98, login : user, Password : walouwlouuwlaou



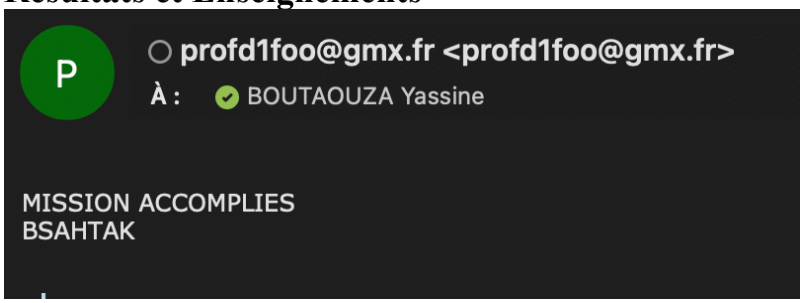
4. Analyse des Résultats

La phase d'analyse a permis de recueillir différentes métriques:



- Taux d'ouverture du message
- Taux de clic sur le lien
- Pourcentage d'utilisateurs ayant saisi leurs identifiants
- Informations techniques (adresses IP, agents utilisateurs)

Résultats et Enseignements



Cette simulation a permis de mettre en évidence:

1. **La facilité de création** d'une campagne de phishing convaincante
2. **L'importance de la vérification des URL** avant de cliquer
3. **Les indicateurs de suspicion** à rechercher dans les messages
4. **L'efficacité des formations de sensibilisation** pour réduire les risques

Ip : 85.69.173.98, login : user, Password : walouwlouuwlaou

Conclusion

Ce projet de simulation de phishing éducatif illustre parfaitement pourquoi la sensibilisation des utilisateurs constitue l'un des piliers fondamentaux de la cybersécurité. En comprenant les techniques utilisées par les attaquants, les utilisateurs peuvent développer les réflexes nécessaires pour se protéger efficacement.

La cybersécurité étant un domaine en constante évolution, ce type d'exercice pratique s'avère indispensable pour maintenir un niveau de vigilance adapté face aux menaces actuelles.

Ce projet a été réalisé dans un cadre académique contrôlé et avec l'autorisation explicite de toutes les parties concernées, conformément aux principes éthiques de la sécurité informatique.