MOUHAMADOU MOKHTAR THIAM
24/12/25

RAPPORT TECHNIQUE

Rapport de Simulation de Phishing avec ZPHISHER

I. Introduction

Le phishing est l'une des attaques les plus courantes dans le domaine de la cybersécurité. Il consiste à tromper un utilisateur en se faisant passer pour une entité de confiance afin de lui soutirer des informations sensibles (identifiants, mots de passe, etc.).

Ce rapport présente une simulation réalisée avec **Zphisher**, un outil open-source permettant de cloner des pages de connexion populaires pour tester la réaction des utilisateurs face à un hameçonnage.

II. Objectifs de la simulation

- Comprendre le fonctionnement d'une attaque de phishing.
- Tester la réaction d'un utilisateur cible face à un faux site de connexion.

III. Méthodologie

a. Outil utilisé : Zphisher

Zphisher est un script automatisé de phishing permettant de :

- Cloner facilement des sites de connexion (Facebook, Gmail, Microsoft, etc.)
- Générer un lien à envoyer à la cible (via Ngrok, Localhost ou Serveo)
- Capturer l'adresse IP de la victime
- Sauvegarder automatiquement les identifiants et mots de passe saisis

b. Étapes de la simulation :

1. Lancement de Zphisher sur un environnement Linux.
2. Sélection d'un service à cloner (ex. : Facebook).
3. Génération d'un lien via **Ngrok** pour un accès distant.

RAPPORT TECHNIQUE

4. Partage du lien avec une personne cible (dans un cadre pédagogique et simulé).
5. Capture des données saisies par la victime (IP, identifiant, mot de passe).

---

4. Résultats

Extrait de la capture d'écran (console Zphisher) :

- IP détectée :
  `154.124.201.111`
  `34.83.203.92`
- Identifiants récupérés :
  - **Nom d'utilisateur** : `matar`
  - **Mot de passe** : `1111111111`
- Fichiers générés :
  - `auth/ip.txt` : enregistrement des adresses IP
  - `auth/usernames.dat` : enregistrement des identifiants

IV. Analyse des résultats

- **Succès de l'attaque** : L'utilisateur a été trompé et a saisi ses identifiants sur la fausse page de connexion.
- **Comportement observé** : Aucune vérification de l'URL ou du certificat HTTPS n'a été faite par la cible.
- **Temps de réponse rapide** : Ce qui montre que l'attaque aurait pu être exploitée en temps réel par un attaquant.

7. Conclusion

Cette simulation avec Zphisher démontre qu'une attaque de phishing peut facilement duper un utilisateur non averti. Elle confirme la nécessité de renforcer la **culture de cybersécurité**, d'autant plus dans un environnement éducatif ou professionnel.