République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Oran1, Faculté des Sciences Exactes et Appliquées Département d'Informatique

MASTER 1 SÉCURITÉ INFORMATIQUE

Module : Piratage éthique et défense des systèmes

Projet 4 Campagne de phishing ethique avec Gophish

SOMMAIRE

1. Résumé exécutif

Ce projet décrit la mise en place d'une **campagne de phishing éthique simulée**, réalisée dans un environnement local sécurisé grâce à la plateforme Gophish. L'objectif principal était d'**observer le comportement des utilisateurs face à des emails frauduleux**, de repérer les failles humaines en cybersécurité et de proposer des recommandations pour mieux se protéger.

Les résultats ont montré que **la majorité des utilisateurs a interagi avec les messages**, ce qui met en évidence le besoin urgent de **sensibilisation et de renforcement des mesures de sécurité**.

2. Méthodologie

2.1 Environnement et topologie

La campagne a été exécutée **dans un environnement isolé**, sans connexion à Internet, afin d'assurer un cadre sûr et éthique.

- **Système d'exploitation** : Kali Linux (dans la machine virtuelle vbox)
- **Plateforme de phishing** : Gophish
- **Serveur SMTP local** : MailHog
- **Navigateur web** : simulation des actions des utilisateurs (FireFox)

2.2 Outils utilisés

Outil	Utilisation
Kali Linux	Système pour les tests et simulations
Gophish	Création et gestion de la campagne
Python	Automatisation via API
MailHog	Serveur SMTP local
Navigateur	Firefox installé sur Kali Linux, utilisé pour simuler le comportement des utilisateurs.

2.3 Configuration de la campagne Gophish

2.3.1 Email template

Cette interface permet de définir le contenu des courriels envoyés dans le cadre de la campagne.

Les modèles ont été conçus pour simuler des messages réalistes afin d'analyser la réaction des utilisateurs.

- **Nom** : EH_template
- **Contenu HTML** :

```
<h3>Mise à jour urgente</h3>
<p>Veuillez vérifier votre compte immédiatement.</p>
<a href="{{.URL}}">Cliquez ici</a>
```

Analyse :

- Message court et urgent
- Incitation directe à l'action
- Lien dynamique vers la page de capture

2.3.2 Landing Page

La landing page correspond à la page vers laquelle l'utilisateur est redirigé après le clic sur l'e-mail.

Elle permet d'observer et d'analyser les interactions des utilisateurs dans un contexte contrôlé.

- **Nom** : EH_landing_page
- **Contenu HTML** :

```
<!DOCTYPE html>
<html lang="fr">
<head>
<meta charset="UTF-8"/>
<title>Vérification du compte</title>
<style>
  body { font-family: Arial; background: #f2f2f2; }
  .container { width: 360px; margin: 100px auto; background: white; padding: 25px; border-radius: 6px; box-shadow: 0 0 10px rgba(0,0,0,0.1); }
</style>
</head>
<body>
<div class="container">
  <h2>Vérification du compte</h2>
```

```
  <form method="POST" action="">
    <label>Adresse e-mail</label>
    <input type="email" name="email" required/>
    <label>Mot de passe</label>
    <input type="password" name="password" required/>
    <input type="submit" value="Se connecter"/>
  </form>
</div>
</body>
</html>
```

- **Paramètres de capture :**
  - Capture des informations saisies (oui).
  - Collecte des mots de passe (oui).

2.3.3 Sending Profile

Le sending profile définit les paramètres d'envoi des courriels.

MailHog est utilisé comme serveur SMTP local afin d'assurer un envoi sécurisé et éthique.

- **Nom** : MailHog
- **Type** : SMTP
- **Serveur** : 127.0.0.1
- **Port** : 1025
- **Expéditeur** : admin@test.localhost

2.3.4 Users & groupes

Cette interface permet de gérer les utilisateurs ciblés en les organisant en groupes.

Les groupes facilitent la gestion de la campagne et l'analyse des résultats.

- **Nom du groupe** : groupe_EH
- **Fichier CSV** :

email	first_name	last_name
user1@test.local	sara	sarah
user2@test.local	safia	sofie
user3@test.local	Nebia	nebiaa

2.3.5 Automatisation de la campagne par script Python (launch_phish.py)

Afin de faciliter la gestion de la campagne et de réduire les interventions manuelles, une partie du projet a été automatisée à l'aide d'un script Python développé spécifiquement pour ce travail.

Ce script exploite l'API REST de la plateforme Gophish et permet d'orchestrer plusieurs étapes clés de la campagne de phishing éthique.

Fonctionnalités principales du script

Le script Python implémente les fonctionnalités suivantes :

- Connexion à l'API Gophish à l'aide d'une clé d'authentification ;
- Création automatique de la campagne (nom, durée et paramètres généraux) ;
- Association des éléments de la campagne :
    - modèle d'email ;
    - page de destination (landing page) ;
    - profil d'envoi SMTP (via MailHog) ;
    - groupe d'utilisateurs ciblés ;
- Lancement automatique de la campagne sans intervention manuelle ;
- Récupération des statistiques générées par Gophish (clics sur les liens, soumissions de formulaires).

Cette automatisation permet d'assurer une meilleure reproductibilité des campagnes, de réduire les erreurs humaines et d'optimiser le temps nécessaire aux phases de test et d'analyse.

2.3.6 Gestion des dépendances (requirements.txt)

Un fichier requirements.txt a été utilisé afin de définir les dépendances logicielles nécessaires à l'exécution du script d'automatisation développé dans le cadre de ce projet.

Dans ce fichier, la bibliothèque Python requests (version 2.31.0) est spécifiée, car elle permet d'assurer la communication via le protocole HTTP entre le script Python et l'API REST de la plateforme Gophish. Cette bibliothèque est notamment utilisée pour l'envoi de requêtes HTTP (GET et POST) permettant la création de campagnes de phishing ainsi que la récupération des résultats associés.

L’utilisation de ce fichier facilite l’installation de l’environnement requis et garantit la portabilité ainsi que la reproductibilité du projet sur différentes machines.

‘’ Les fichiers sources du projet ainsi qu’une vidéo de démonstration, illustrant l’exécution de la campagne et les tests réalisés, ont été fournis séparément dans le dépôt GitHub.

Le présent rapport se concentre principalement sur la description des fonctionnalités implémentées et l’analyse des résultats obtenus.”

3. Résultats

3.1 Indicateurs clés

Indicateur	Valeur
Nombre d’utilisateurs	3
Nombre de clics	2
Taux de clics	66 %

3.2 Analyse comportementale

- La majorité des utilisateurs ont **cliqué rapidement sur le lien**.
- Aucun n’a vérifié l’URL réelle avant de cliquer.
- L’effet d’**urgence** a clairement influencé leurs décisions.

Remarque : le facteur humain reste le maillon faible face aux attaques de phishing.

4. Recommandations

4.1 Formation à la cyber sécurité

- Sensibilisation aux emails suspects.
- Apprentissage des signaux d’alerte.
- Exercices pratiques réguliers.
- Mise à jour continue des connaissances sur les nouvelles menaces.
- Création de guides ou fiches pratiques pour les employés.
- Organisation de sessions interactives avec des études de cas réels.
- Encouragement de la culture de cyber sécurité au sein de l’organisation.

4.2 Mise en place de l'authentification multifactorielle (MFA)

- Réduction des risques en cas de compromission.
- Sécurisation renforcée des comptes sensibles.
- Vérification régulière de la configuration MFA.
- Intégration de la MFA sur tous les services critiques.
- Sensibilisation des utilisateurs à l'importance de la MFA et de la gestion sécurisée des dispositifs.
- Suivi des incidents et ajustement des règles de sécurité si nécessaire.

4.3 Simulations régulières

- Campagnes de phishing tous les trimestres.
- Suivi de l'évolution du taux de clics.
- Analyse des résultats pour identifier les points faibles.
- Sessions de feedback pour améliorer la vigilance des utilisateurs.
- Adaptation progressive des scénarios pour couvrir de nouvelles menaces.
- Documentation des résultats pour évaluer l'efficacité de la formation et des mesures de sécurité.

5. Cadre éthique et légal

- La simulation a été réalisée uniquement sur les membres du groupe.
- Elle s'est déroulée dans un environnement local et sécurisé.
- Aucune donnée réelle n'a été utilisée.
- Respect strict de la confidentialité et de la vie privée des participants.
- Conformité avec les régulations et normes de cybersécurité en vigueur.

Conformité : cette expérience respecte la **Loi 19-05 sur la protection des données personnelles**.

6. Conclusion

Cette simulation montre que les attaques exploitant l'**urgence restent très efficaces**. Le projet souligne l'importance d'une approche combinant **sensibilisation humaine et mesures techniques** pour renforcer la sécurité globale.