الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة وهران 1 أحمد بن بلة
Université Oran 1
كلية العلوم الدقيقة والتطبيقية
Faculté des sciences exactes et appliquées

Dec 2025

## Projet 7 :

# Piratage éthique et défense des systèmes

## Rapport : Analyse forensique post-phishing

---

Réalisé par :
Selmi Yousra
Fellah Farah
Fatah Ahlem

Spécialité :
Sécurité Informatique

# 1. Résumé exécutif

Ce projet consiste à réaliser une analyse **forensique post-phishing** sur un email malveillant simulé, généré localement, dans le but d'identifier les Indicateurs de Compromission (IOCs) sans jamais ouvrir ou exécuter le contenu suspect.

L'analyse a permis de détecter plusieurs éléments caractéristiques d'une attaque de phishing, notamment des **adresses IP suspectes**, **des mots-clés** à caractère urgent et sécuritaire, ainsi qu'un expéditeur usurpant l'identité d'une entreprise légitime par typosquatting.

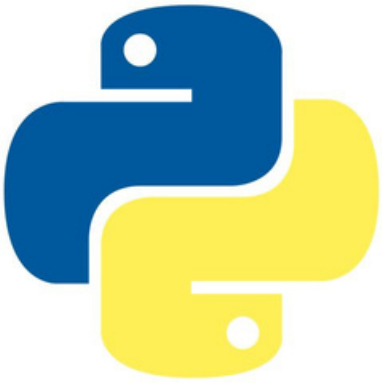
L'outil développé **automatise l'analyse et génère un rapport technique** structuré, reproduisant le travail réel d'un analyste SOC confronté à un email signalé par un employé.

# 2. Description du dataset

## 2.1 Environnement et topologie


* Machine virtuelle locale : **Kali Linux**
* Aucune connexion réseau sortante pendant l'analyse
* Email analysé sous forme de fichier texte brut (.eml)
* Pièces jointes générées localement par le groupe

Cette approche garantit une analyse sécurisée, contrôlée et conforme aux exigences éthiques.



## 2.2 Outils et technologies utilisés

* Python 3
* Bibliothèques standard : email, re, os, subprocess
* Génération de rapport : reportlab
* Analyse de métadonnées : exiftool (appel via subprocess)

# 2. Description du dataset

## 2.3 Étapes de l'analyse

1. Lecture du fichier phishing_email.eml
2. Parsing des headers pour extraire les IP sources
3. Analyse de l'expéditeur (From)
4. Analyse du corps HTML de l'email
5. Détection de mots-clés de phishing
6. Extraction et stockage des pièces jointes
7. Analyse des métadonnées des fichiers joints
8. Génération automatique du rapport PDF

# 3. Résultats de l'analyse

## 3.1 Analyse des headers

L'analyse des champs Received a permis d'identifier plusieurs adresses IP présentes dans les en-têtes de l'email, indiquant l'origine ou le transit du message.

## 3.2 Analyse de l'expéditeur

L'adresse email de l'expéditeur utilise un domaine trompeur imitant une entreprise légitime, ce qui correspond à une technique de typosquatting, fréquemment utilisée dans les campagnes de phishing.

## 3.3 Analyse du contenu

Le corps de l'email contient des mots-clés à forte charge émotionnelle tels que (urgent, verify, security, login), incitant l'utilisateur à agir rapidement sans réflexion.

## 4. Recommandations de sécurité

À la suite de cette analyse, les mesures suivantes sont recommandées :

* Sensibiliser les employés à la vérification des domaines d'expédition
* Mettre en place des règles de filtrage basées sur les mots-clés suspects
* Bloquer les adresses IP malveillantes au niveau du pare-feu
* Analyser systématiquement les pièces jointes dans un environnement sandbox
* Renforcer les politiques de sécurité email (SPF, DKIM, DMARC)

## 5. Conclusion

Le projet a permis de développer un outil automatisé capable d'analyser efficacement un email malveillant simulé et d'en extraire les principaux indicateurs de compromission.
L'approche adoptée reflète les pratiques réelles d'un analyste SOC en situation post-incident et répond pleinement aux objectifs pédagogiques du Projet

# Merci !