Projet 9 – Piratage éthique et défense des systèmes
Comparaison d’outils de reconnaissance OSINT

UEM112 – Sécurité Informatique
Implémentation Python vs outils professionnels

1. Résumé exécutif

Ce projet vise à concevoir une implémentation Python maison de fonctions fondamentales d'OSINT (WHOIS, résolution DNS et collecte d'emails professionnels) afin de les comparer à des outils professionnels tels que Maltego et Recon-ng. L'objectif est de démystifier le fonctionnement interne de ces outils, souvent considérés comme des boîtes noires, tout en respectant strictement les principes du piratage éthique et la réglementation en vigueur.

2. Méthodologie

2.1 Environnement et topologie

Les tests ont été réalisés sur une machine virtuelle locale fonctionnant sous Kali Linux. Les cibles analysées sont exclusivement des domaines publics open-source (ex. : wordpress.org, apache.org).

2.2 Outils et bibliothèques

Les bibliothèques Python utilisées sont : whois pour les requêtes WHOIS, dnspython pour la résolution DNS avancée, requests pour l'accès à l'API Hunter.io, et reportlab pour la génération du rapport PDF.

2.3 Étapes d'exécution

Chaque module est exécuté indépendamment afin de collecter les données. Les temps d'exécution sont mesurés et comparés aux résultats obtenus via les outils standards en ligne de commande ou interfaces web.

3. Résultats – Tableau comparatif

Critère	Implémentation maison	Outils professionnels
WHOIS	Informations clés via librairie	Données enrichies
DNS	A, MX, NS, TXT	Résolution complète + graphes
Emails	Hunter.io (API gratuite)	Sources multiples
Vitesse	Rapide (local)	Variable
Précision	Bonne	Très élevée
Transparence	Totale	Limitée (boîte noire)

4. Analyse éthique

Le projet respecte strictement les principes du piratage éthique et la Loi algérienne 19-05. Aucun scan actif, aucune exploitation de vulnérabilités et aucun domaine sensible n’ont été ciblés. Toutes les données collectées proviennent de sources publiques et d’APIs autorisées.

5. Recommandations et perspectives

5.1 Choix de l’outil

Une implémentation maison est recommandée pour l’apprentissage, les audits légers et les scripts personnalisés. Les outils professionnels sont plus adaptés aux investigations OSINT complexes et à grande échelle.

5.2 Extensions possibles

Le module peut être étendu par l’ajout de la résolution CNAME, des enregistrements SPF et DMARC, ou encore l’intégration d’autres APIs OSINT publiques.