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
Capacités WHOIS	Données essentielles via librairie	Données enrichies + corrélation multi-sources
Capacités DNS	A, MX, NS, TXT via dnspython	Résolution étendue + visualisation
Collecte d’emails	API Hunter.io (clé gratuite)	Sources multiples et agrégation
Précision	Bonne (dépend des APIs publiques)	Très élevée (cross-check automatique)
Vitesse WHOIS	~0.4 s	~1–2 s
Vitesse DNS	~0.2 s	~0.8 s
Vitesse Emails	~0.6 s	~1.5 s
Transparence	Totale (pas de boîte noire)	Limitée
Scalabilité	Moyenne	Élevée

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 Quand utiliser une implémentation maison vs un outil professionnel

• **Implémentation maison :** adaptée à l’apprentissage, compréhension des protocoles, contrôle total, scripts automatisés pour audits légers, respect strict des règles éthiques et contraintes budgétaires.

• **Outils professionnels :** recommandés pour les investigations OSINT complexes, analyse à grande échelle, visualisation avancée, gain de temps et usage professionnel/industriel.

En résumé, l’implémentation maison est idéale pour l’apprentissage et les audits ponctuels, alors que les outils professionnels sont plus adaptés aux investigations à grande échelle et aux contextes opérationnels nécessitant précision et enrichissement des données.

5.3 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.