Exercice Pratique : Analyse de WHOIS avec et sans protection

Objectif pédagogique :

- Apprendre à lire et interpréter les informations d'un enregistrement WHOIS,
- Identifier si un domaine utilise une protection de vie privée,
- Comparer les informations disponibles dans les deux cas,
- Déduire les risques ou avantages selon les types d'informations visibles.

Mise en situation :

Vous êtes un auditeur cybersécurité chargé d'une **analyse de surface (reconnaissance passive)** sur deux noms de domaine publics.

Votre mission : **Comparer les données WHOIS** d'un site **non protégé** et d'un site **protégé**, et produire un **mini-rapport d'analyse**.

Étapes à suivre :

1. Rechercher le WHOIS du domaine suivant :

Cas 1 : Domaine non protégé

Domaine : `unice.fr`
Lien : https://whois.domaintools.com/unice.fr

Relever ces informations :

- Nom du propriétaire (ou organisation)
- Adresse email ou téléphone
- Date de création et de mise à jour
- Adresse IP du site
- Hébergeur (registrar)

2. Rechercher le WHOIS d'un domaine protégé

Domaine : `examplexyz.org` (ou un site avec WhoisGuard activé)
Exemple : https://whois.domaintools.com/examplexyz.org *(ou n'importe quel domaine affichant WhoisGuard)*

Relever :

- Le type de protection utilisée (WhoisGuard, Privacy Protect, etc.)
- L'email affiché (protégé ? redirigé ?)
- Le registrar utilisé
- Les serveurs DNS
- Est-ce qu'on peut deviner l'hébergeur réel ?

Livrable attendu : Mini-Rapport en tableau comparatif

Représente tes résultats comme ceci :

Élément	Domaine NON protégé (`unice.fr`)	Domaine PROTÉGÉ (`examplexyz.org`)
Organisation	Université Côte d'Azur	WhoisGuard Inc.
Email	contact@unice.fr	xyz123@whoisguard.com
Création	1995-01-23	2022-08-15
Propriétaire visible ?	Oui	Non
Protection WHOIS	Non	WhoisGuard
DNS	ns1.unice.fr	ns1.digitalocean.com

Questions de réflexion (à inclure dans le rapport) :

1. Pourquoi certaines entreprises préfèrent **ne pas masquer** leurs infos ?
2. Quels sont les **risques** si les emails et noms sont visibles dans WHOIS ?
3. Dans quel cas est-ce **utile pour un attaquant** de consulter WHOIS ?
4. Quels outils peuvent être utilisés en complément de WHOIS pour la reconnaissance ?
5. Le domaine protégé est-il **totalement anonyme** ? Peut-on en apprendre plus autrement ?

Outils recommandés :

- https://whois.domaintools.com
- https://www.whois.com/whois/
- https://archive.org/web/
- https://haveibeenpwned.com