Intro à l'OSINT

Jeanne D'Hack CTF - 2025

Orangius

H3110 W0r1D !

JEANNE DHACK CTF

Avertissement Légal

L'OSINT doit être utilisé uniquement dans un cadre légal et éthique.

✖ Ne jamais utiliser ces techniques pour espionner, harceler ou obtenir des informations personnelles sans consentement.
⚠ **L'utilisation abusive d'outils et de méthologie d'OSINT peut entraîner des conséquences légales graves** (atteinte à la vie privée, usurpation d'identité, etc.).

Ce cours et le challenge associé sont conçus **uniquement à des fins pédagogiques**. Toute utilisation dans un contexte réel sans autorisation/mandat est **fortement déconseillée**.

Qu'est ce que l'OSINT, ou ROSO (oui c'est moche) en français?

> OSINT pour Open Source Intelligence, est une méthode de collecte et d'analyse de données provenant de sources ouvertes, c'est-à-dire accessibles à tous.
> ROSO pour Renseignement d'Origine Source Ouverte.

Peut être effectué sur différentes cibles:

- Personnes
- Entreprises
- Organisations
- Gouvernements
- Etc.

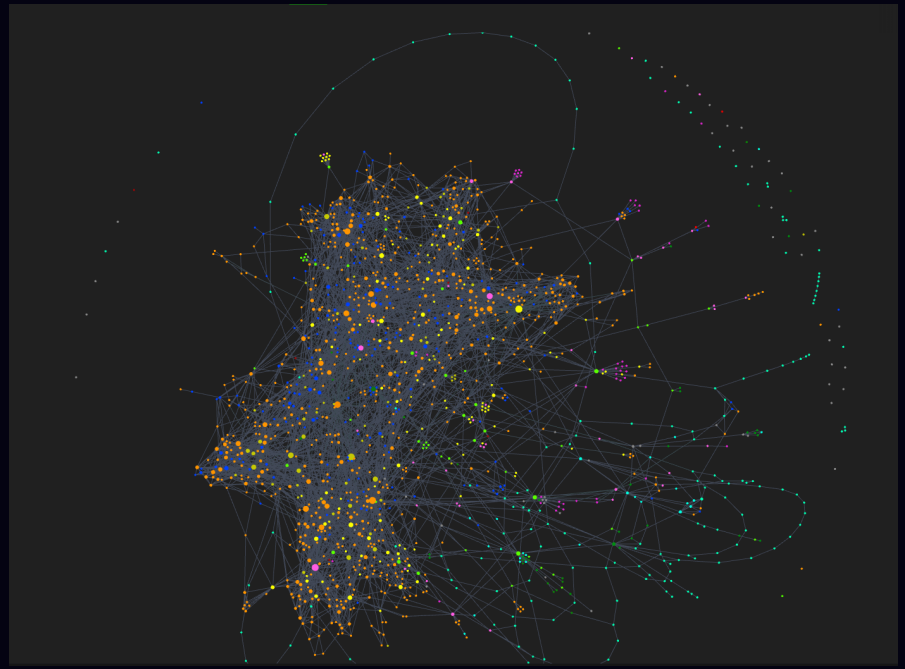
En utilisant des sources ouvertes:

- Sites web
- Réseaux sociaux
- Forums
- Geo-localisation
- Informations d'images
- Etc.

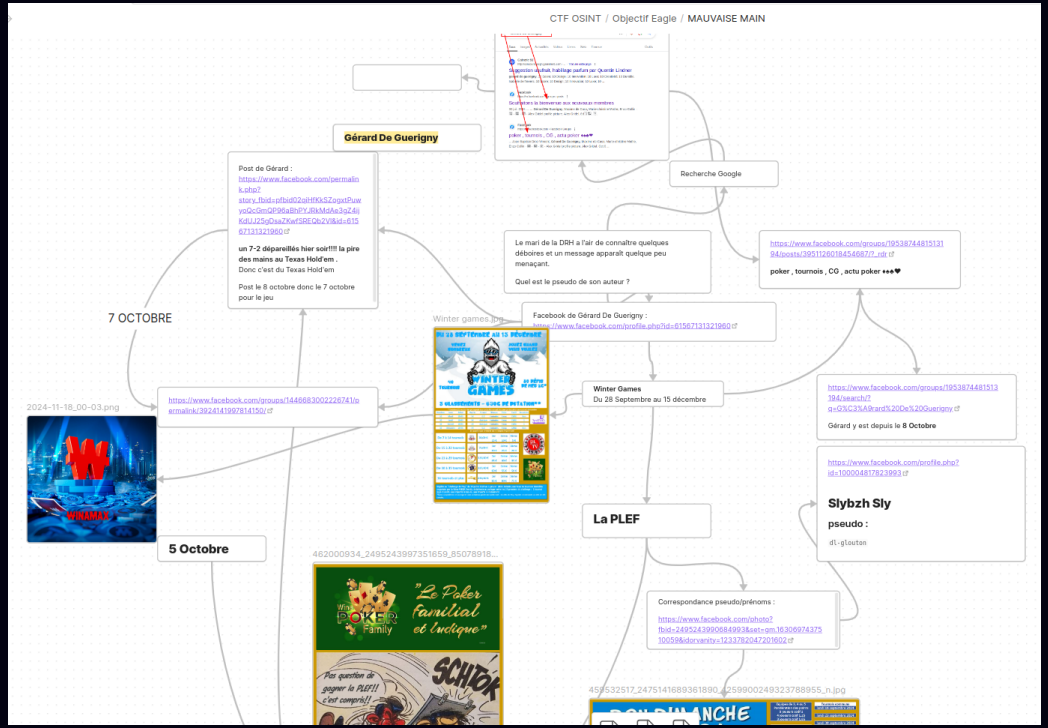
🔍 Comment faire de l'OSINT ?

L'OSINT est une discipline qui nécessite :

- 🛠 **Des compétences techniques** et la maîtrise d'outils spécifiques.
- **Une approche méthodique et organisée** pour éviter de se perdre dans la masse d’informations collectées.
- **Des outils de prise de notes** pour structurer ses recherches. (#TeamObsidian)



Organisation selon moi



🏷️ Sous-catégories dans l'OSINT

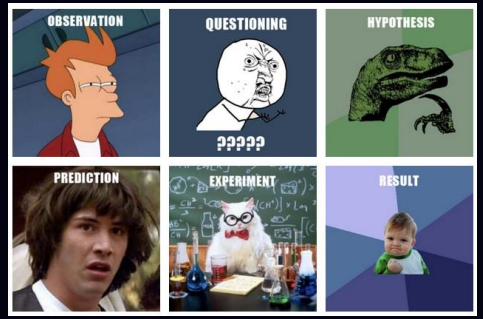
L'OSINT peut être divisé en plusieurs domaines spécialisés :

- **SOCMINT (Social Media Intelligence)** → Exploitation des réseaux sociaux (Twitter, Facebook, Instagram...).
- **GEOINT (Geospatial Intelligence)** → Analyse d'images satellites et de données de géolocalisation.
- **IMINT (Imagery Intelligence)** → Étude et analyse d'images et de vidéos.
- **SIGINT (Signals Intelligence)** → Surveillance des communications et des signaux (radio, WiFi, Bluetooth...).
- **HUMINT (Human Intelligence)** → Renseignement obtenu directement auprès d'individus.
- **TECHINT (Technical Intelligence)** → Recherche d'informations techniques sur les systèmes et technologies.

🕵️‍♂️ **Chaque branche a ses propres outils et méthodologies !**

Méthodologie générique en OSINT

- **Collecte d'informations**
- **Analyse des informations**
- **Corrélation des informations**
- **Rapport d'OSINT**
- Mouais c'est plutôt ça en fait :



Les outils les plus connus en OSINT

Nom	Développeur(s)	Spécificité
Maltego	Paterva	Visualisation de liens et d'entités
Shodan	John Matherly	Moteur de recherche d'appareils connectés
Spiderfoot	Steve Micallef	Exploration automatique de sources ouvertes
theHarvester	Christian Martorella	Collecte d'emails, sous-domaines, noms, etc.
OSINT Framework	Justin Nordine	Répertoire d'outils OSINT
Recon-ng	Tim Tomes	Framework modulaire pour la collecte d'informations
Google Dorks	Google	Techniques de recherche avancée sur Google
Sherlock	Sherlock Project	Recherche de comptes sur les réseaux sociaux
Wayback Machine	Internet Archive	Archive de pages web
...	...	...

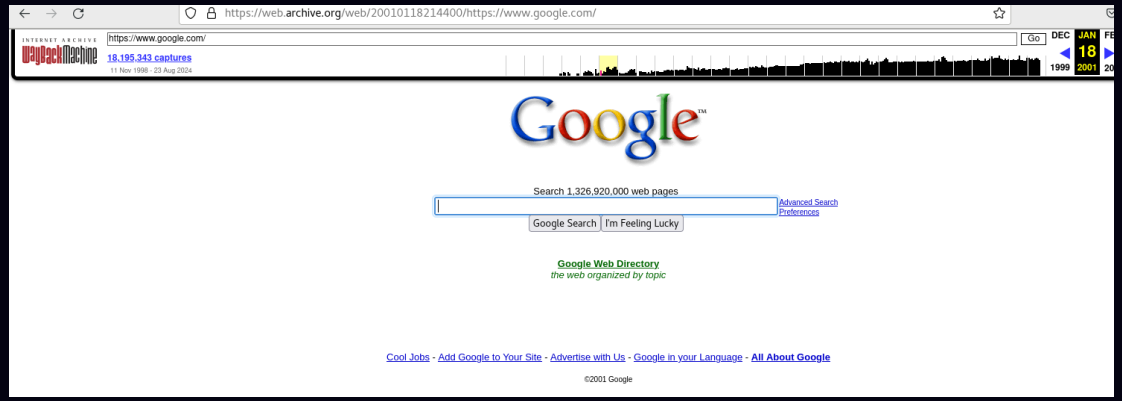
Ressources :

- https://bellingcat.gitbook.io/toolkit
- https://osintfr.com/en/tools/
- https://github.com/jivoi/awesome-osint
- https://osintframework.com/
- https://ozint.eu/

Utilisation de Wayback Machine

> [Wayback Machine](https://archive.org/web/) est un service en ligne qui permet de consulter des pages web archivées.
> Il est utile pour retrouver des informations sur des sites web qui ont été supprimés ou modifiés.

Exemple : Page google en 2001



Exemple avec le challenge Learning

Exemple avec le challenge Learning

Mission Votre mission, en tant qu'enquêteur OSINT, est de retrouver **l'adresse mail** d'une cible à partir d'une **photo** supposément liée à elle.

Une fois l'adresse e-mail identifiée, vous pourrez également découvrir un flag sous la forme `JDHACK{...}`, qui vous permettra de réussir le challenge.

Analyse de l'image

Pas de pseudo, d'informations concernant la cible. Une recherche Google ne mène à rien.

- Ok, ça s'arrête là alors ?
- Et non ! Nous avons une image, donc nous allons effectuer de l'IMINT (Étude et analyse d'images)
- L'image a des meta données, dont des données EXIF. Nous pouvons voir rapidement ces données avec l'outil `exiftool` comme ceci :
- `exiftool ./img/conv.jpg`

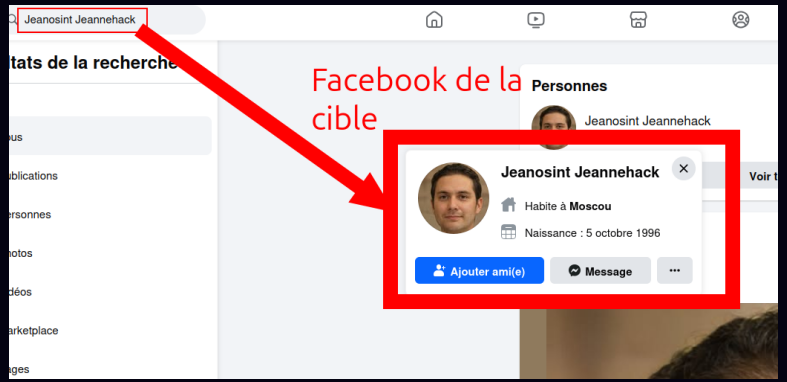
Analyse d'image (IMINT)

```
exiftool ./img/conv.jpg
```

Recherche sur les réseaux (SOCMINT)

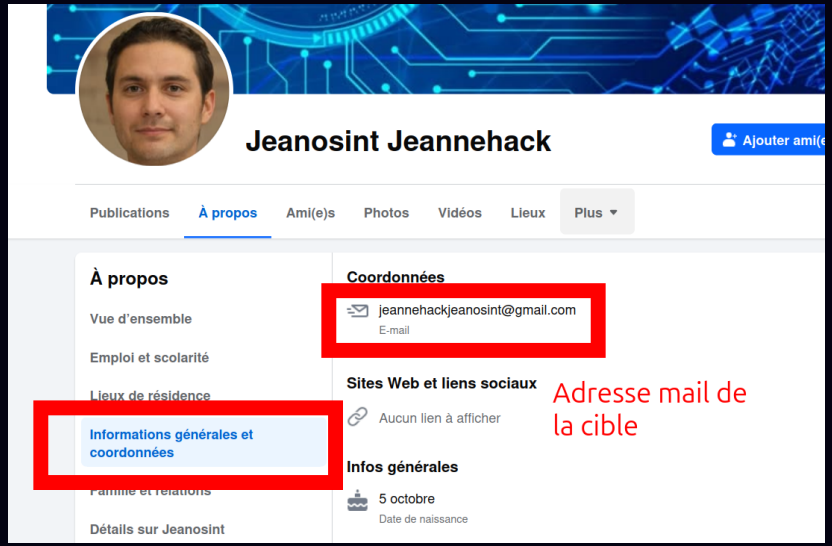
Nous avons donc obtenu le prénom et le nom de la cible : `Jeanosint Jeannehack`.

Nous pouvons donc rechercher notre cible sur Internet et spécialement sur les réseaux sociaux. En cherchant bien nous trouvons son compte sur Facebook :



Bravo !!

Et bam on obtient l'adresse mail du fameux Jeanosint Jeannehack :



On a donc : jeannehackjeanosint@gmail.com

Je vous laisse trouver le flag pour réussir le challenge ;)

A vous de jouer!

Vous êtes maintenant prêts pour effectuer les challenges de la catégorie OSINT dans le CTF !!

Questions?