

Mireille GUETCHO

COMPTE RENDU DU TP CONTRE-MESURE OSINT

Lien du TP :

<https://docs.google.com/document/d/10aZ3a0XK584NdVfMQrwTQTZjMmlFKzLoQCp6-hxYcDk/edit?usp=sharing>

REPONSES AUX QUESTIONS

1

A. Google Dorks ou Google Dorking est une technique avancée de recherche qui utilise des opérations spécifiques pour extraire des informations sensibles ou cachées à partir de Google. De ce fait, cela affine les résultats et permet de trouver les données qui ne sont pas forcément visibles à première vue.

Les Informations que nous pouvons trouver dans Google Dorks :

- Informations sensibles et fichiers exposés
- Pages d'administration et accès non sécurisés
- Caméras de surveillances et systèmes ouverts
- Répertoires ouverts et fichiers indexés
- Bases de données exposées
- Emails et contacts
- Vulnérabilités et exploits

B

Google search results for "mireille guetcho".

LinkedIn · mireille guetcho
Plus de 160 abonnés

mireille guetcho - Stagiaire en Système information ...
France · Stagiaire en Système information Système Réseau · ITIC Paris
Étudiante en SERVICES INFORMATIQUES AUX ORGANISATIONS à ITIC PARIS · Expérience Paris · Formation : ITIC Paris · Lieu : France · 152 ...

Facebook
<https://www.facebook.com/mireille.guetcho>

Mireille Guetcho
Mireille Guetcho is on Facebook. Join Facebook to connect with Mireille Guetcho and others you know. Facebook gives people the power to share and...

RocketReach
<https://rocketreach.co/mireille-g...> · Traduire cette page

Mireille Guetcho Email - Stagiaire @ Sophie Barat
Mireille Guetcho, based in France, is currently a Stagiaire at Groupe Scolaire Sophie Barat M...

Google search results for "mireille guetcho instagram".

Instagram · mireillegagne1
Plus de 1,8 k abonnés

Mireille Gagné (@mireillegagne1)
Autrice + passionnée de littérature + chasse et pêche + tricot. Ne mange pas de gluten. Crédit p
Émilie Dumais. www.mireillegagne.com.
Termes manquants : guetehe | Afficher les résultats avec : guetcho

Instagram · mireilleguerin95
Plus de 690 abonnés

Mireille Guérin (@mireilleguerin95)
696 Followers, 433 Following, 78 Posts - Mireille Guérin (@mireilleguerin95) on Instagram: "Ar
contemporain Fils et couleurs licier cartonnier Art textile ...
Termes manquants : guetehe | Afficher les résultats avec : guetcho

Instagram · mireillegueniot
Plus de 30 abonnés

Mireille Guéniot (@mireillegueniot)

Google search results for "mireille guetcho @gmail.com".

Search bar: mireille guetcho @gmail.com

Navigation: Tous Images Vidéos Actualités Maps Livres Web Plus

Results:

- LinkedIn · mireille guetcho**
Plus de 160 abonnés
mireille guetcho - Stagiaire en Système information ...
France · Stagiaire en Système information Système Réseau · ITIC Paris
Étudiante en SERVICES INFORMATIQUES AUX ORGANISATIONS à ITIC PARIS · Expérience Paris · Formation : ITIC Paris · Lieu : France · 152 ...
- Facebook**
<https://www.facebook.com/mireille.guetcho>
Mireille Guetcho
Mireille Guetcho is on Facebook. Join Facebook to connect with Mireille Guetcho and others you know. Facebook gives people the power to share and...
Termes manquants : @gmail | Afficher les résultats avec : @gmail.
- Google Help**
<https://support.google.com/mail/thread/ouverture-s...>
Ouverture sur un message et non sur la boîte de réception

Google search results for "hackaday".

Search bar: hackaday

Navigation: Tous Vidéos Images Actualités Web Maps Livres Plus

Results:

- Hackaday**
<https://hackaday.com> · Traduire cette page
Hackaday | Fresh Hacks Every Day
Hackaday. Primary Menu. Home · Blog · Hackaday.io · Tindie · Hackaday Prize · Submit · About
Search for: February 13, 2025. What Happens If You Die In Space?
- Blog**
Skip to content. Logo · Hackaday. Primary Menu. Home · Blog ...
- Fresh Hacks Every Day | Page 2**
Here at Hackaday, we pride ourselves on bringing you the ...
- Projects**
Hackaday. Primary Menu. Home · Blog · Hackaday.io · Tindie ...

← → ↻ google.fr/search?q=hackaday+blog&sca_esv=... ☆

hackaday blog

Tous Vidéos Images Actualités Web Livres Maps Plus

 Hackaday
https://hackaday.com › blog · Traduire cette page

Blog | Hackaday | Fresh Hacks Every Day

Skip to content. Logo · Hackaday. Primary Menu. Home · Blog · Hackaday.io · Tindie · Hackaday
· Submit · About. Search for: February 13, 2025. A ...

Blog
A short bio about yourself · 3 example daily posts written in ...

Blog | Hackaday
Hackaday. Primary Menu. Home · Blog · Hackaday.io ... Blog ...

Older posts
Copyright © 2025 | Hackaday, Hack A Day, and the Skull and ...

← → ↻ google.fr/search?q=hackaday+prize&sca_esv=... ☆

hackaday prize

Tous Images Vidéos Actualités Web Maps Livres Plus

Conseil : Affichez les résultats en français. Vous pouvez aussi en savoir plus sur le f
par langue.

 Hackaday Prize
https://prize.supplyframe.com · Traduire cette page

2023 Hackaday Prize

What is the Hackaday Prize? A global hardware design challenge focused on widespread and
impactful innovation. For ten years, the Hackaday Prize has offered ...

 Hackaday
https://hackaday.com › category · Traduire cette page

The Hackaday Prize

7 nov. 2023 — As finalists, each of these projects has been awarded \$500 to help further their
development. But perhaps more importantly, they are now ...

C

Les informations accessibles sur **Instagram, Twitter (X) et LinkedIn** varient en fonction de la nature de chaque plateforme et des paramètres de confidentialité des utilisateurs. Nous pouvons avoir:

Sur Instagram

Plateforme principalement axée sur le partage d'images et de vidéos

- Nom et pseudo
- Photo de profil et biographie
- Publications (photos, vidéos, carrousels)
- Stories publiques et Highlights
- Reels publics
- Nombre d'abonnés et d'abonnements
- Commentaires et likes sur les publications publiques
- Localisation (si activée par l'utilisateur)
- Hashtags utilisés
- Recommandations via l'algorithme (explore, suggestions)

Sur Twitter (X)

Plateforme axée sur les messages courts (tweets) et les débats d'actualité

- Nom et pseudo (@handle)
- Photo de profil et bannière
- Biographie et lien éventuel (site, autre réseau)
- Tweets (publics, avec texte, images, vidéos, GIFs, liens)
- Retweets et likes publics
- Réponses aux tweets
- Listes publiques créées par l'utilisateur
- Nombre d'abonnés et d'abonnements
- Espace Twitter (si public)

Sur LinkedIn

Plateforme professionnelle axée sur le networking et l'emploi. Les informations accessibles publiquement (selon les paramètres de confidentialité) comprennent :

- Nom et photo de profil
- Titre professionnel (ex. : "Marketing Manager chez [Entreprise]")
- Résumé et description du profil
- Expériences professionnelles et entreprises associées
- Formations et diplômes
- Compétences et recommandations
- Publications et articles rédigés sur LinkedIn
- Nombre de connexions (souvent affiché si +500)
- Interactions (likes, commentaires, partages de publications publiques)

D

E

Le **WHOIS** est un protocole permettant d'obtenir des informations sur un nom de domaine, une adresse IP ou un réseau. Il est utilisé pour interroger les bases de données des registrars (bureaux d'enregistrement) et obtenir des détails sur le propriétaire du domaine, la date d'enregistrement, les contacts administratifs et techniques, ainsi que les serveurs DNS associés.

Nous pouvons trouver comme informations :

- Informations sur le propriétaire :

(Nom et prénom, Organisation ou entreprise, Adresse postale, Adresse e-mail, Numéro de téléphone)

- Détails d'enregistrement du domaine

(Nom du bureau d'enregistrement exemple : GoDaddy, OVH, Namecheap; Date de création du domaine ; Date d'expiration ; Dernière mise à jour).

- Contacts associés au domaine

(Contact administratif ; Contact technique ; Contact de facturation)

- Serveurs DNS associés

(Serveurs de noms (NS) utilisés pour la résolution DNS)

- Statut du domaine

(Actif, en attente de suppression, transférable ou protégé).

F

TheHarvester est un outil open-source utilisé pour la collecte d'informations (OSINT – Open Source Intelligence) sur des noms de domaine, des entreprises ou des adresses IP. Il permet de récupérer des données publiques depuis diverses sources en ligne pour réaliser du renseignement offensif (pentesting) ou défensif (audit de sécurité).

Nous pouvons trouver comme informations :

- Adresses e-mail associées à un domaine
- Sous-domaines et domaines associés
- Adresses IP et blocs IP liés au domaine
- Serveurs et hôtes détectés
- Employés et contacts

(via les moteurs de recherche et les réseaux sociaux)

- Fichiers et documents sensibles

(via Google Dorks)

- Informations sur les services DNS et les enregistrements MX

G

Le **Shodan** est un moteur de recherche spécialisé qui explore Internet pour recenser et indexer les appareils connectés. Contrairement à Google, qui indexe des pages web, Shodan scanne les services et infrastructures exposés (serveurs, caméras, routeurs, systèmes SCADA, etc.).

Nous pouvons trouver comme informations :

- Adresses IP publiques d'appareils connectés
- Ports ouverts et services actifs

(HTTP, SSH, FTP, etc.)

- Bannières des services

(version du serveur, OS, certificats SSL, etc.)

- Périphériques connectés

(caméras IP, routeurs, serveurs, systèmes industriels SCADA)

- Failles de sécurité

(appareils utilisant des versions vulnérables)

- Certificats SSL/TLS des sites web
- Données de géolocalisation des appareils

2

A

Un attaquant peut utiliser **Google Hacking (Google Dorking)** pour collecter des informations sensibles exposées involontairement sur Internet. Ces données peuvent ensuite être exploitées pour mener des attaques contre des sites web, des entreprises ou des individus.

B

Les réseaux sociaux sont une **mine d'or d'informations** pour les attaquants. Grâce aux données publiquement accessibles (photos, posts, relations, localisation, etc.), un attaquant peut :

- Mener des attaques ciblées (phishing, ingénierie sociale)
- Usurper une identité et créer de faux profils
- Collecter des informations sensibles pour du chantage ou de l'espionnage
- Accéder à des comptes protégés via des réponses aux questions de sécurité

- Analyser les habitudes et la vie privée d'une cible

C

WHOIS étant une base de données qui permet de récupérer des informations sur un nom de domaine, comme le propriétaire, les contacts, les dates d'enregistrement et les serveurs DNS.

Un attaquant peut utiliser les informations collectées pour :

- Mener des attaques d'ingénierie sociale et du phishing
- Usurper une identité et compromettre un domaine
- Rechercher des vulnérabilités sur les serveurs DNS et emails
- Lancer une attaque par force brute ou par DDoS

D

Un attaquant peut exploiter les données trouvées sur TheHarvester pour :

- Mener des attaques de phishing et d'ingénierie sociale
- Identifier des sous-domaines et services vulnérables
- Récupérer des emails et usernames pour des attaques de brute-force
- Trouver des fuites de données et des vulnérabilités exploitables

E

Shodan est un moteur de recherche spécialisé qui permet de trouver des appareils connectés à Internet.

Un attaquant peut exploiter les informations collectées pour :

- Rechercher des services vulnérables
- Lancer des attaques sur des ports ouverts
- Accéder à des bases de données non sécurisées
- Prendre le contrôle d'objets connectés
- Exploiter des failles dans des infrastructures critiques

3

F

Pour se protéger contre les attaques via Google, nous devons :

- Éviter de stocker des fichiers sensibles en accès public
- Désactiver l'indexation des répertoires dans les fichiers **.htaccess** ou **robots.txt**
- Utiliser des mots de passe robustes et une authentification à deux facteurs (2FA)
- Mettre à jour régulièrement ses logiciels et services
- Vérifier son exposition avec des outils comme TheHarvester ou Google Dorks

G

Pour se protéger contre les attaques via les réseaux sociaux, nous devons :

- Paramétrer ses comptes en privé et limiter l'accès aux infos personnelles
- Utiliser un mot de passe unique et robuste pour chaque service
- Ne pas partager d'informations sensibles sur des posts publics
- Ne pas cliquer sur des liens suspects envoyés par message
- Se méfier des demandes d'argent ou d'accès inhabituelles
- Faire une recherche sur soi-même (Google Dorking) pour voir ce qui est exposé

H

Pour se protéger contre les attaques via Whois, nous devons :

- Activer la protection WHOIS Privacy chez le registrar pour masquer les infos personnelles
- Utiliser une adresse e-mail dédiée et protégée pour l'enregistrement du domaine
- Sécuriser les serveurs DNS avec DNSSEC
- Limiter les services exposés en désactivant les sous-domaines inutiles
- Mettre à jour les serveurs et activer des protections contre le DDoS

I

Pour se protéger contre TheHarvester, nous devons :

- Masquer les informations sensibles sur le **WHOIS**
- Limiter la visibilité des employés sur LinkedIn
- Utiliser des emails uniques et privés pour l'administration des domaines
- Bloquer les scans automatiques via un bon paramétrage du DNS

- Mettre en place une politique stricte contre le phishing

J

Pour se protéger contre les attaques via Shodan, nous devons :

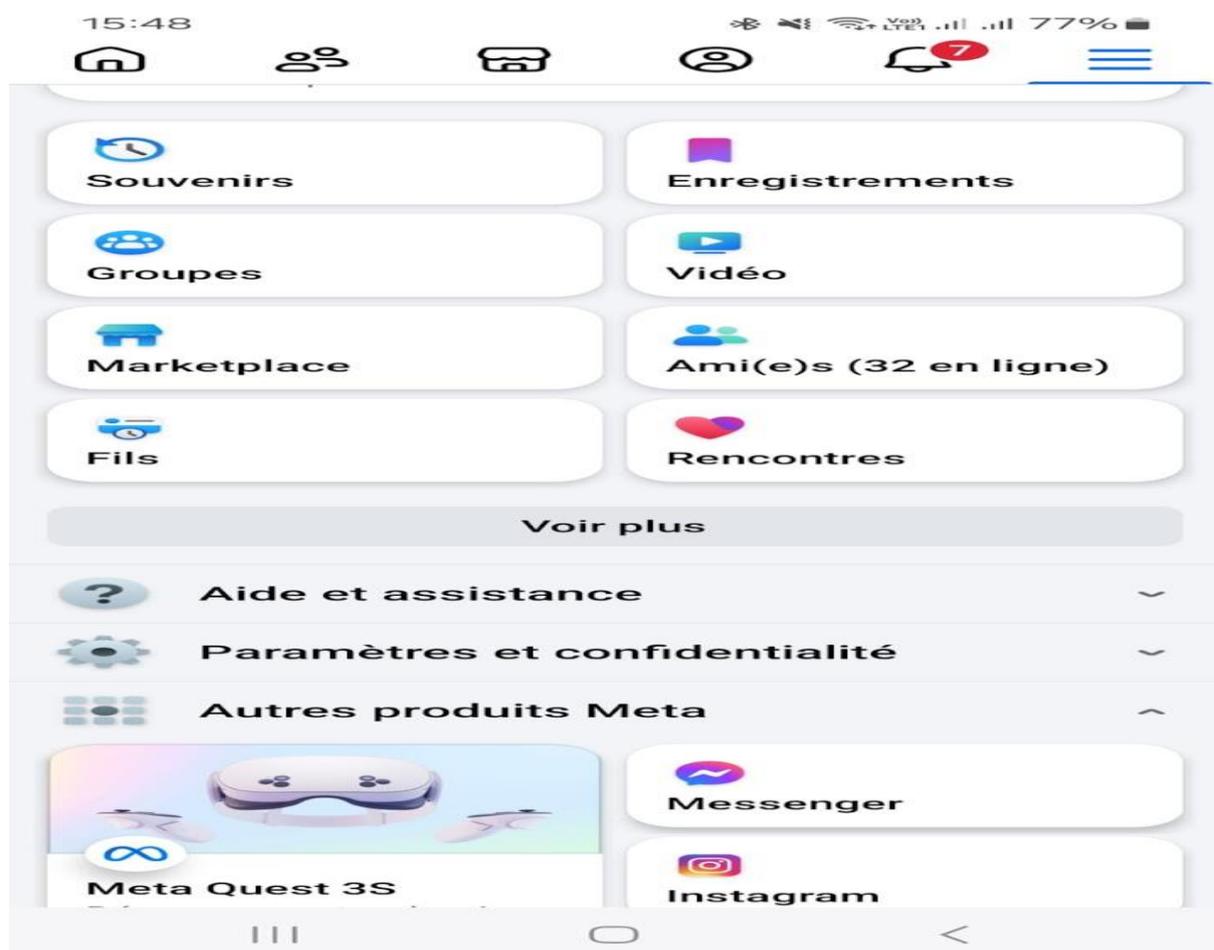
- Fermer les ports inutiles sur les serveurs et appareils IoT
- Configurer un pare-feu et filtrer les adresses IP autorisées
- Désactiver les accès par défaut et exiger une authentification forte
- Utiliser un VPN pour masquer les services accessibles publiquement
- Surveiller son propre réseau avec Shodan pour détecter les failles

4

A. Configuration des paramètres de confidentialités sur Facebook

Pour le faire, nous allons suivre les étapes suivantes :

Paramètres et confidentialité → Paramètres → Confidentialité





Nous allons ensuite ajuster les options suivantes :

- Qui peut voir tes publications ? → "Moi uniquement" ou "Amis"
- Qui peut voir ta liste d'amis ? → "Moi uniquement"
- Qui peut te trouver avec ton email ou numéro ? → "Moi uniquement"
- Autoriser les moteurs de recherche à afficher ton profil ? → Désactive cette option



Rechercher dans les paramètres

Meta

Espace Comptes

Gérez vos expériences partagées et vos paramètres de comptes sur l'ensemble des technologies Meta.

-  Informations personnelles
-  Mot de passe et sécurité
-  Préférences publicitaires
-  Vérification

[En voir plus dans l'Espace Comptes](#)

Outils et ressources

Nos outils vous aident à contrôler et gérer votre confidentialité.

-  Assistance confidentialité
-  Supervision parentale
-  Paramètres d'audience par défaut

Préférences

Personnalisez votre expérience sur Facebook.

-  Préférences en matière de contenu
-  Préférences des réactions





Assistance confidentialité

Nous vous aiderons à prendre les bonnes décisions pour les paramètres de votre compte.

Par quelle rubrique voulez-vous commencer ?



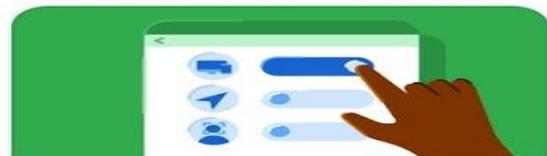
Qui peut voir ce que vous partagez



Comment protéger votre compte



Comment il est possible de vous trouver sur Facebook



Les paramètres de vos données sur Facebook



Vos préférences publicitaires sur Facebook



< Informations du profil

Veillez vérifier ces informations sur votre profil et choisir qui peut les voir. Votre profil peut contenir plus d'informations que ce qui apparaît ici.

Numéro de téléphone

07 61 02 14 02

 Moi uniquement ▾

+36 30 725 1793

 Moi uniquement ▾

Adresse e-mail

guetchomir
eille@yahoo
.fr

 Moi uniquement ▾

Date de naissance

9 septembre

 Ami(e)s et leur... ▾

1992

 Ami(e)s et leur... ▾

Ville d'origine

Kekem, Littoral, Cameroon

 Public ▾

Ville actuelle



Suivant



< Informations du profil

Date de naissance

9 septembre

👥 Ami(e)s et leur... ▾

1992

👥 Ami(e)s et leur... ▾

Ville d'origine

Kekem, Littoral,
Cameroon

🔒 Moi uniquement

Ville actuelle

Yaoundé

🔒 Moi uniquement

Scolarité

université de yaoundé
1

🔒 Moi uniquement ▾

Lycée de Kékem

🔒 Moi uniquement ▾

Amis et personnes/Pages suivies

Qui peut voir votre
liste d'ami(e)s sur
votre profil ?

🔒 Moi uniquement ▾

Qui peut voir les personnes,
Pages et listes que vous
suivez ?

🌐 Public ▾



Suivant





Audience par défaut

Choisissez votre audience par défaut

Le fait de choisir une audience par défaut définit automatiquement l'audience du contenu que vous partagez, mais vous pouvez à tout moment la modifier pour une publication, une story ou un reel spécifique.

Vous pouvez modifier vos paramètres à tout moment.



Public

Tout le monde peut voir ce que vous partagez et interagir avec votre contenu public.



Ami(e)s

Seul(e)s vos ami(e)s peuvent voir ce que vous partagez. Si vous créez une publication publique, seul(e)s vos ami(e)s pourront la commenter.



Personnalisée · Vos paramètres actuels

Choisissez manuellement qui peut voir ce que vous partagez et interagir avec votre contenu public.



[Besoin d'aide pour choisir ?](#)

Suivant



15:58

75%



Paramètres personnalisés

Terminé

Qui peut voir vos futures publications ?

Moi uniquement



Qui peut voir vos stories ?

Ami(e)s



Qui peut voir vos reels ?

Public



Autoriser les autres à partager vos stories publiques dans leur story personnelle ?



Autoriser d'autres personnes à partager vos reels dans leurs stories ?



Qui peut commenter vos publications publiques ?

Public



Informations de profil publiques

Ami(e)s



Qui peut voir les personnes, Pages et listes que vous suivez ?

Public



Voulez-vous que les moteurs de recherche en dehors de Facebook affichent un lien vers votre profil ?



B

Lorsqu'un enregistrement de nom de domaine est fait , les informations personnelles (nom, adresse, email, téléphone) sont stockées dans la base de données **WHOIS** et peuvent être **publiques** par défaut.

Il est possible de masquer les informations avec un service de protection **WHOIS** (appelé aussi **WHOIS Privacy Protection**).

- Vérifier si les infos sont publiques sur un site WHOIS
- Activer la protection WHOIS depuis ton registrar (gratuit ou payant)
- Choisir un registrar qui inclut WHOIS Privacy (ex: Namecheap, Google Domains)
- Utiliser un service de proxy WHOIS si le registrar ne propose pas l'option
- Faire attention aux domaines qui n'acceptent pas la protection WHOIS (ex: .fr, .us)

C