**ETHICAL HACKING**

## Module 1 :  Introduction to Ethical Hacking

## Les terminologies essentielles

### *Définition*Hack value

C'est une notion de**hacking** qui veut dire **quelque chose qui vaut la peine ou intéressant**. C'est aussi une raison ou une motivation pour dépenser des efforts pour un objectif apparemment inutile, le fait que le **but accompli est un hack**.

### *Définition*Vulnérabilité

C'est l'existence d'une faiblesse, d'une conception ou d'une erreur de mise en œuvre qui peut conduire à un événement inattendu compromettant la sécurité du système.

### *Définition*Exploit

C'est une **violation de la sécurité du système informatique par des vulnérabilités**. C'est également un logiciel ou une séquence de code qui profite d'une vulnérabilité pour compromettre la sécurité d'un système

### *Définition*Payload

C'est une partie d'un code d'exploitation qui exécute des actions malveillantes prévues, telles que la destruction, la création de **backdoors** (porte arrière).

### *Définition*zero-day (0 day) attack

C'est une attaque qui **exploite les vulnérabilités des applications informatiques** avant que le développeur de logiciel ne **publie un patch** ou ne « patche »la vulnérabilité.

### *Définition*Daisy chaining

Il s'agit d'accéder à un réseau et / ou **un ordinateur, puis d'utiliser les mêmes informations pour accéder à plusieurs réseaux** et ordinateurs contenant des informations utiles.

### *Définition*Doxing

Publier des informations personnellement identifiables sur un individu collectées à partir de bases de données disponibles publiquement et des médias sociaux ...

### *Définition*Bot

C'est une application ou logiciel qui peut être contrôlé à distance pour exécuter ou automatiser des tâches prédéfinies

## Les éléments sécurité l'information

### *Définition*

La sécurité de l'information est un état de bien-être de l'information et de l'infrastructure dans laquelle **la possibilité de vol, de manipulation et d'interruption d'informations et de services est faible ou tolérable**.

### *Méthode*Confidentialité

La confidentialité est le caractère réservé d'une information ou d'un traitement dont l**'accès est limité aux seules personnes admises à la ou le connaître**.

Assurez-vous que l'information est accessible **uniquement aux personnes autorisées à avoir accès**.

La fonction  « Confidentialité »traite du chiffrement permettant d'assurer que les données ne seront accessibles, lors de leur échange ou de leur stockage, que par les destinataires de ces données.

### *Méthode*Intégrité

La **fiabilité des données ou des ressources** en termes de prévention des modifications incorrectes et non autorisées.

Les données de la communication n'ont pas été altérées.

### *Méthode*Disponibilité

## Assurez-vous que le les systèmes responsables de la livraison, du stockage et du traitement des informations sont accessibles **lorsque les utilisateurs autorisés le demandent**.

Les acteurs de la communication accèdent aux données dans de bonnes conditions.

### *Méthode*Authenticité

L'authentification a pour but de vérifier l'identité d'une personne ou d'une machine afin que celle-ci puisse accéder à un système d'information.

### *Méthode*Non répudiation

**Garantir** que l'expéditeur d'un message ne peut plus tard nier avoir envoyé le message et que le destinataire ne peut pas refuser d'avoir reçu le message.

## Motifs, buts et objectifs des attaques de la sécurité du SI

### *Méthode*Attaque

**Attaques** = **Motif (But)** + **Méthode** +**Vulnérabilité**

### Motif

Le motif vient de l'idée que**le système cible ou la cible d'évaluation stocke ou traite** quelque chose de précieux et cela entraîne une menace d'attaque contre le système

### *Méthode*

Les attaquants essaient divers outils et attaquent en utilisant leurs compétences et techniques pour **exploiter les vulnérabilités** dans un système informatique ou une politique de sécurité et des contrôles pour atteindre leurs objectifs et satisfaire leur motivation

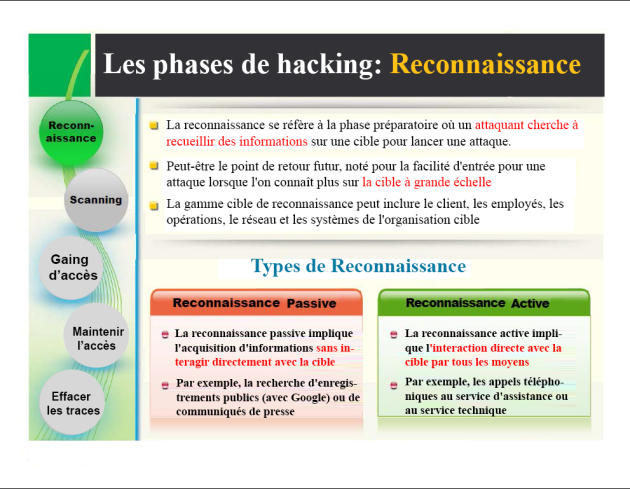
### Motifs liés aux attaques de la sécurité de l'information

* *Perturbant la continuité des activités*
* *Vol de l'information*
* *Manipulation des données*
* *Créer la peur et le chaos en perturbant les infrastructures critiques*
* *Propagation de croyances religieuses ou politiques*
* *Atteindre les objectifs militaires de l’État*
* *Réputation dommageable de la cible*
* *Prendre une revanche*

**Les phases de hacking**

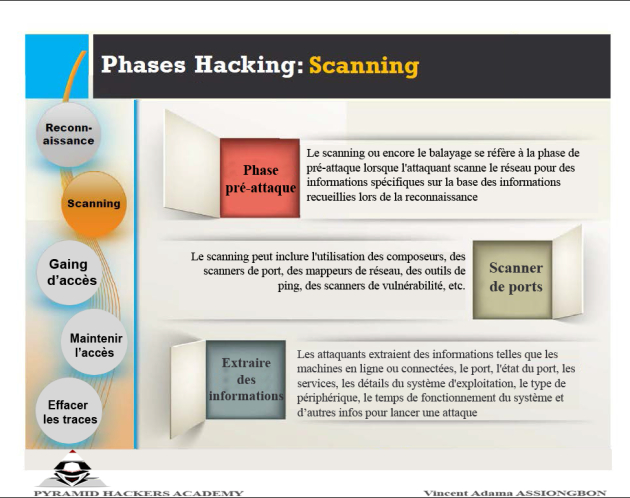
* [La phase de reconnaissance](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_20.html) :

La reconnaissance se réfère à la phase préparatoire où un**attaquant cherche à recueillir des informations sur une cible** pour lancer une attaque



* [Phase scanning](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_21.html):

Le **scanning** ou encore le balayage se réfère à la phase de pré-attaque lorsque l'attaquant scanne le réseau pour des informations spécifiques sur la base des informations recueillies lors de la reconnaissance. C'est une phase pré-attaque.



* [Phase de gain d'accès](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_22.html) :

Le**gain d'accès** se réfère au point où le hacker ou l'attaquant obtient l'accès au système d'exploitation ou à l'application sur l'ordinateur ou sur le réseau

* [Phase de maintient d'accès](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_23.html) :

Le maintient de l'accès se réfère à la phase où l'attaquant tente de maintenir l'accès de manière continuelle sur le système de la cible en installant un rootkit ou un trojan (cheval de troie). De ce fait à chaque fois que la **victime redémarre ou lance son système**, **elle se connecte automatiquement sur la machine** de l'attaquant.

* [Phase de suppression de trace](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_24.html) :

La suppression ou l'effacement de trace se réfère à des activités menées par un attaquant **pour masquer ou effacer les actes malveillants.**

Une fois que le système est compromis après avoir maintenu l'accès, les attaquants nettoient leurs traces en effaçant les fichiers log ou fichiers de journalisation.

Fondamental

Les intentions de l'attaquant sont les suivantes :

* **action continue au système de la victime**
* **action inaperçue et non détectée**
* **suppression de preuves susceptibles de conduire à des poursuites**

### *Complément*

L'attaquant remplace les données du serveur par ses données , supprime les fichiers log d'application et tout fichier compromettant pour éviter tout soupçon.

Fondamental

Les hackers couvrent toujours les pistes pour cacher leur identité.

## Module 2 :  Footprinting and reconnaissance

## Concept de footprinting

### *Définition*

Le premier pas vers Ethical hacking est Footprinting. Footprinting est la collecte de toutes les informations possibles concernant la cible et le réseau cible.

### Objectifs Footprinting

Les principaux objectifs de Footprinting sont:

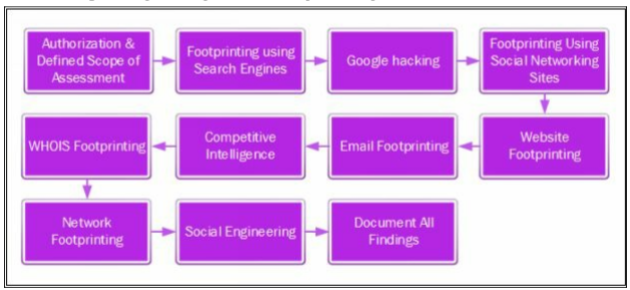
1. Connaître la posture de sécurité
2. Réduire la zone de mise au point
3. Identifier les vulnérabilités
4. Dessinez une carte du réseau

## Méthodologie de Footprinting

### *Méthode*

Ce n'est pas grave d'obtenir des informations sur qui que ce soit car Internet, les réseaux sociaux, les sites officiels et d'autres ressources ont beaucoup d'informations non sensibles sur leurs utilisateurs, mais une collection d'informations peut remplir les exigences d'un attaquant et l'attaquant peut rassembler assez d'informations par un petit effort. Voici plus souvent les techniques utilisées par les pirates informatiques:

* Footprinting au travers des moteurs de recherche
* Footprinting grâce aux techniques avancées de piratage de Google
* Footprinting au travers des sites de réseautage social
* Footprinting au travers de sites Web
* Footprinting par courrier électronique
* Footprinting grâce à la veille concurrentielle
* Footprinting via WHOIS
* Footprinting via DNS
* Footprinting au travers du réseau
* Footprinting grâce à l'ingénierie sociale



## Footprinting utilisant les techniques avancées de Google hacking

### Opérateurs de recherche avancée Google

Certaines options avancées peuvent être utilisées pour rechercher un sujet spécifique à l'aide de moteurs de recherche. Ces opérateurs de recherche avancée ont rendu la recherche plus appropriée et centrée sur un certain sujet. Les opérateurs de recherche avancée par Google sont:

|  |  |
| --- | --- |
| **Advanced Search Operators/Opérateurs de recherche avancée** | **Description** |
| site : | Rechercher le résultat dans le domaine donné. |
| related : | Rechercher des pages Web similaires. |
| cache : | Afficher les pages Web stockées dans le cache |
| link : | Lister les sites Web ayant un lien vers une page Web spécifique. |
| allintext : | Rechercher des sites Web contenant un mot clé spécifique. |
| intext : | Rechercher des documents contenant un mot clé spécifique |
| allintitle : | Rechercher des sites Web contenant un mot clé spécifique dans le titre |
| intitle : | Rechercher des documents contenant un mot clé spécifique dans le titre |
| allinurl : | Rechercher des sites Web contenant un mot clé spécifique dans une URL |
| inurl : | Rechercher des documents contenant un mot clé spécifique dans une URL |

Pour la recherche avancée Google, vous pouvez également accéder à l'URL suivante: <https://www.google.com/advanced_search>

## Google Hacking Database (GHDB)/Base de données de Google hacking

Google Hacking, Google Dorking est une combinaison de techniques de hacking permettant de détecter les failles de sécurité au sein du réseau et des systèmes d'une entreprise à l'aide de la recherche Google et d'autres applications fournies par Google.

Google hacking popularisé par Johnny Long. Il a classé les requêtes dans une base de données appelée Google Hacking Database (GHDB). Cette base de données catégorisée de requêtes est conçue pour découvrir les informations. Cette information peut être sensible et non disponible publiquement. Google Hacking est utilisé pour accélérer les recherches. Comme le montre la figure, sur [www.exploit-db.com](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/www.exploit-db.com), vous pouvez rechercher GHDB ou parcourir la catégorie GHDB. De même que [www.hackersforcharity.org](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/www.hackersforcharity.org) est également une plate-forme en ligne pour GHDB.

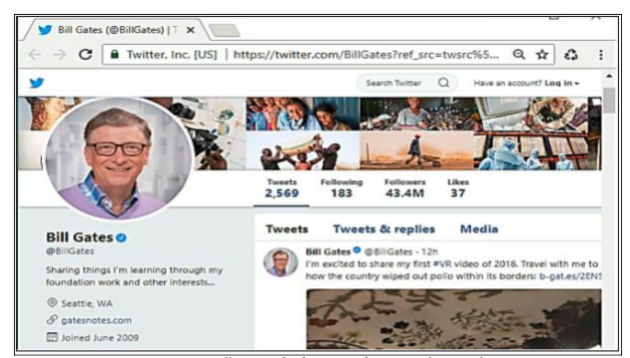
Entrez l'URL suivante: [https://www.exploit-db.com/google-hacking-database](https://www.exploit-db.com/google-hacking-database/)

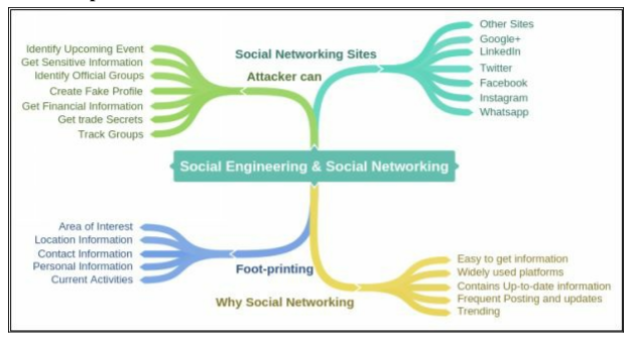
La base de données de Google Hacking fournit les informations mises à jourqui sont utiles pour l'exploitation, telles que les bases, les répertoires sensibles, les fichiers vulnérables, les messages d'erreur, etc.

## Footprinting en utilisant l'ingénierie sociale sur les sites de réseautage social

Le réseautage social est l'une des meilleures sources d'information parmi d'autres. Différents sites de réseaux sociaux populaires et les plus largement utilisés ont rendu très facile la recherche d'une personne, l'information sur une personne, y compris ses informations personnelles de base ainsi que certaines informations sensibles. Les fonctionnalités avancées de ces sites de réseaux sociaux fournissent également des informations actualisées. Un exemple de Footprinting via des sites de réseaux sociaux peut être de trouver quelqu'un sur **Facebook, Twitter, LinkedIn, Instagram** et bien plus encore.

|  |  |  |
| --- | --- | --- |
| **Que font les utilisateurs?** | **Information** | **Ce que l'attaquant obtient** |
| Les gens maintiennent leur profil | * Photo de la cible * Numéro de contact * Adresses mail * Date de naissance * Emplacement * Détails de travail | * Informations personnelles sur une cible, notamment des informations personnelles, une photo, etc. * Ingénierie sociale |
| Les personnes mettent à jour leur statut | * Informations personnelles les plus récentes * Lieu le plus récent * Informations sur la famille et les amis * Activités et intérêts * Informations relatives à la technologie * Informations sur les événements à venir | * Informations relatives à la plate-forme et à la technologie. * Emplacement cible. * Liste des Employés / Amis / Famille. * Nature de l'entreprise |





## Quelques outils de footprinting

### *Exemple*Maltego

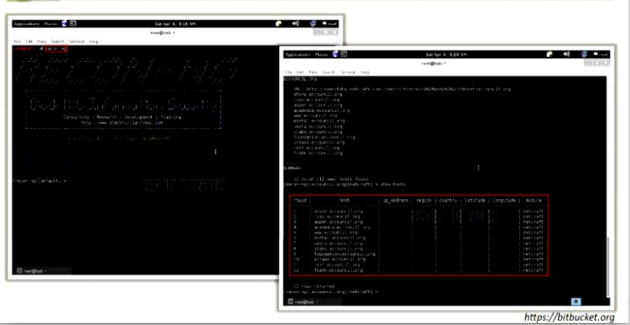
**Maltego** est un programme qui peut étre utilisé pour déterminer les relations et les liens réels entre les groupes de

personnes (réseaux sociaux), les entreprises, les organisations, les sites Internet, l'infrastructure Internet, les phrases, les documents et les fichiers



### *Exemple*Recon-ng

**Recon-ng** est un framework de reconnaissance web avec des modules indépendants, une interaction avec la base de données, des fonctions de commodité intégrées, une aide interactive et la complétion des commandes, qui fournit un environnement dans lequel la reconnaissance web open source peut étre réalisée.



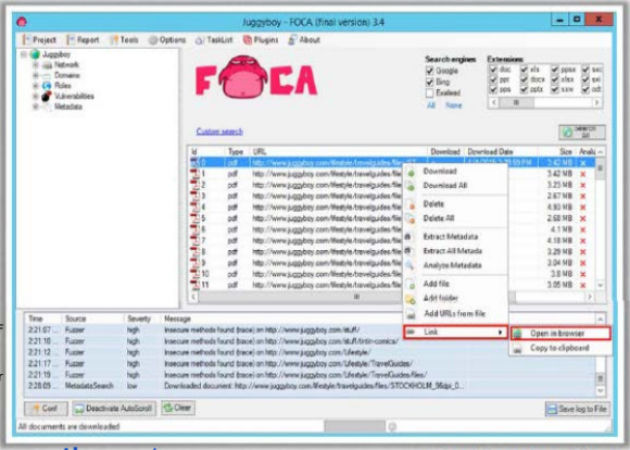
### *Exemple*FOCA

**FOCA** (Fingerprinting Organization with Collected Archives) est un outil utilisé principalement pour trouver des métadonnées et des informations cachées dans les documents de ses analyses.

En utilisant FOCA, il est possible d'entreprendre de multiples attaques et techniques d'analyse telles que l'extraction de métadonnées, l'analyse de réseau, l'espionnage DNS, la recherche de proxy, la recherche de répertoires ouverts, etc.

* Il capable d'analyser une grande variété de documents, avec le plus commun étant Microsoft Office, Open Office ou des fichiers PDF, mais il analyse également les fichiers Adobe! InDesign ou SVG, par exemple.
* Ces documents sont recherchés à l'aide de trois moteurs de recherche possibles : Google, Bing et DuckDuckGo. La somme des résultats des trois moteurs équivaut à un grand nombre de documents.
* ll est également possible d'ajouter des fichiers locaux pour extraire les informations EXIF des fichiers graphiques, et une analyse complète des informations découvertes par l'URL est effectuée même avant de télécharger le fichier

[https://www.elevenpaths.com](https://www.elevenpaths.com/)



## Footprinting et contre-mesures

* Restreindre les employés à accéder aux sites de réseaux sociaux à partir du réseau de l'organisation
* Configurer les serveurs Web pour éviter les fuites d'informations
* Éduquez les employés à utiliser des pseudonymes sur les blogs, les groupes et les forums
* Ne pas révéler d'informations critiques dans les communiqués de presse, les rapports annuels, les catalogues de produits, etc...
* Limiter la quantité d'informations que vous publiez sur les sites web ou réseaux sociaux
* Utiliser des techniques de footprinting pour découvrir et supprimer toute information sensible publiquement disponible
* Empêcher les moteurs de recherche de mettre en cache une page Web et d'utiliser des services d'enregistrement anonymes
* Appliquer des politiques de sécurité pour réguler les informations que les employés peuvent révéler à des tiers personnes.
* Mettre à part le DNS interne et externe ou utiliser le DNS divisé et restreindre le transfert de zone aux serveurs autorisés
* Désactiver la liste de répertoires dans les serveurs Web
* Éduquer les employés sur divers trucs et risques d'ingénierie sociale
* Opter pour les services de confidentialité sur la base de données de recherche Whois
* Éviter la reticulation ou la liaison croisée au niveau du domaine pour les actifs critiques
* Chiffrer et mot de passe et protéger les informations sensibles

## Footprinting Penetration Testing

### *Méthode*

Footprinting Pen Testing est utilisé pour **déterminer les informations publiquement disponibles de I'entreprise ou de |'organisation**.

Le testeur/pentester tente de recueillir autant d'informations que possible sur l'organisation cible a partir **d'Internet et d'autres sources accessibles au public**



### *Fondamental*

### Démarrage

### Obtenir une autorisation appropriée

### *Méthode*



Démarrage

Définir la portée de l'évaluation

Effectuer fotprinting des moteurs de recherche--->Utilisez des moteurs de recherche tels que Google, Yahoo! Recherche, Bing, etc .

Effectuez Google Hacking---> Utilisez des outils tels > que GHDB, MetaGoofil, SiteDigger, etc.

### *Méthode*Définir la portée de l'évaluation

* Obtenir I'autorisation appropriée et définir la portée de I'évaluation

### *Méthode*Effectuer fotprinting des moteurs de recherche

* Les moteurs de recherche de reconnaissance tels que **Google, Yahoo! Search, Ask, Bing, Dogpile,Duckduckgo** etc ... pour collecter les informations de lentreprise ou l'organisation cible telles que les détails des employés, les pages de connexion, les portails intranet, etc ... qui aident a effectuer l'ingénierie sociale et d'autres types d'attaques systéme avancées

### *Méthode*Effectuez Google Hacking

Effectuez Google hacking en utilisant des outils tels que **GHDB, MetaGoofil, SiteDigger, etc**.

### *Méthode*Effectuer footprinting sur les sites de réseaux sociaux

Créer une fausse identité sur des sites de réseaux sociaux tels que **Facebook, Linkedin, badoo,** etc.

* Recueillir des informations sur les employés de l'organisation cible a partir de leurs profils personnels sur les sites de réseaux sociaux tels que Facebook, Linkedin, Twitter, Google+, Pinterest, etc ... qui aident a effectuer I'ingénierie sociale.

### *Méthode*Effectuer footprinting sur des sites Web

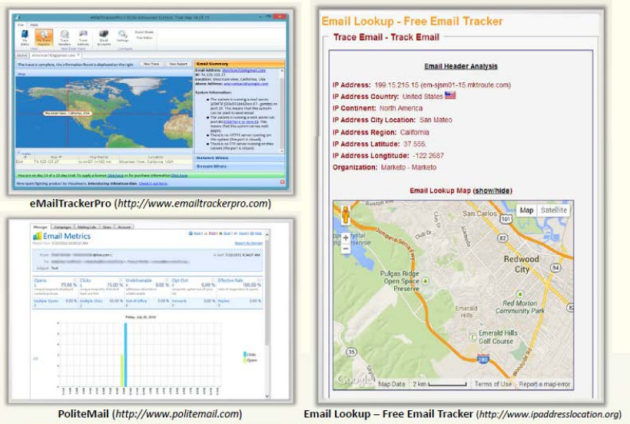
Utilisez des outils tels que le copieur de site Web **HTTrack**, **BlackWidow**, etc.

* Effectuer footprinting du site Web en utilisant des outils tels que le copieur du site Web HTTrack, BlackWidow, Webripper, etc ... pour construire une carte détaillée du site Web et de l'architecture.

### *Méthode*Effectuer footprinting Effectuer email footprinting

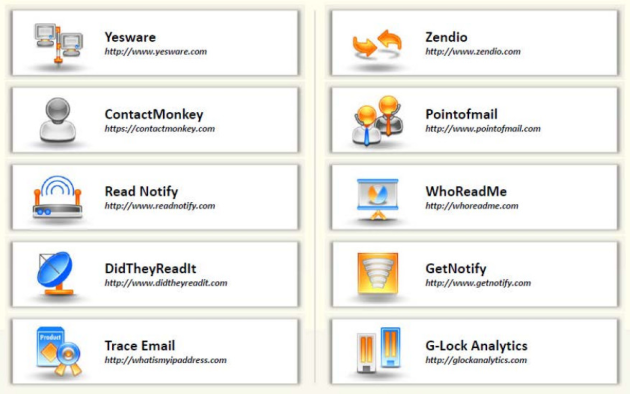
Utilisez des outils tels que **eMailTrackerPro**, **PoliteMail**, etc.

* Effectuer des footprinting digitales l'aide d'outils tels que eMailTrackerPro, PoliteMail, Email Tracker-Tracker gratuit, etc ... pour recueillir des informations sur I'emplacement physique d'un individu pour effectuer l'ingénierie sociale qui peut aider & cartographier le réseau de organisation cible.



[Outils de suivi d'Email](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_35.html)[Informations](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_35.html#footnotesN129)

Autres outils de suivi d'Email



[Autres outils de suivi d'Email](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_35.html)[Informations](https://4gw22br768te-1.unchk.sn/pluginfile.php/8207/mod_imscp/content/1/co/CEHsummary_35.html#footnotesN14c)

### *Méthode*Recueillir de intelligence compétitive

Utilisez des outils tels que **Hoovers**? **LexisNexis**, **Business Wire**, etc.

* Recueillir des renseignements sur la concurrence a l'aide d'outils tels que Hoovers, LexisNexis, Business Wire, etc.

### *Méthode*Efectuer Whois footprinting

Utilisez des outils tels que smartWhois, DomainDossier, Dmitry, etc ..

### *Méthode*Efectuer Whois footprinting

**Efectuez Whois footprinting** en utilisant des outils tels que SmartWhois, Dmitry, etc ... pour

créer une carte détaillée du réseau organisationnel, pour recueillir des informations personnelles qui aident à effectuer l'ingénierie sociale, et pour recueillir d'autres détails de réseau interne, etc ...

### *Méthode*Efectuer DNS footprinting

Efectuez l'empreinte DNS à l'aide d'outils tels que DNSstuf, enregistrements DNS, Dmitry, etc ... pour déterminer les hôtes clés du réseau et efectuer des attaques d'ingénierie sociale.

### *Méthode*Efectuer network footprinting

Efectuez network footprinting en utilisant des outils tel que Path Analyzer Pro, VisualRoute, Network Pinger, etc ... pour créer une carte du réseau de la cible.

### *Méthode*Efectuer l'ingénierie sociale

Mettre en œuvre des techniques d'ingénierie telles que **(eavesdropping, shoulder, surfing et dumpster diving)** l'écoute indiscrète, le surf à l'épaule et la fouille des poubelles qui peuvent aider à recueillir des informations plus critiques sur l'entreprise ou l'organisation cible

À la fin du pen testing documenter tous les résultats

## Modèles de rapport de footprinting pen testing

### *Méthode*

|  |  |
| --- | --- |
| ***Informations obtenues via les moteurs de recherche*** | |
| Détails de l'employé: |  |
| Pages de connexion: |  |
| Portails intranet: |  |
| Plates-formes technologiques: |  |
| Autres: |  |
| **Informations obtenues par la recherche de personnes** | |
| Date de naissance: |  |
| Détails du contact: |  |
| Email ID: |  |
| Photos: |  |
| Autres: |  |

Méthode

|  |  |
| --- | --- |
| Footprinting | |
| **Informations obtenues via Google** | **Informations obtenues grâce au footprinting du site Web** |
| Alertes et vulnérabilités du serveur: | Environnement d'exploitation: |
| Messages d'erreur contenant des informations sensibles: | Structure du système de fichiers: |
| Fichiers contenant des mots de passe: | Plate-formes de script utilisées: |
| Pages contenant des données de réseau ou de vulnérabilité : | Détails du contact: |
| Autres : | Détails du CMS |
|  | Autres : |
| **Informations obtenues via des sites de réseaux sociaux** | **Informations obtenues par footprinting Email** |
| Informations liées au travail: | Adresse IP: |
| Nouvelles et partenaires potentiels de la société cible: | Localisation GPS: |
| Milieux d'éducation et d'emploi: | Système d'authentification utilisé par le serveur de messagerie |

## Module 3 : Scanning network