

La Collecte d'informations

1. Le Foot Printing

Le foot printing est le terme désignant la collecte d'informations sur une entité communicante et toutes les entités liées à cette dernière en possédant un minimum d'informations (nom de domaine ou adresse IP). Le foot printing est considéré comme une approche passive, dans la mesure où on n'entre pas en contact direct avec la cible.

A. Google Hacking

Grâce à la puissance des moteurs de Crawling et d'indexation de Google, il est possible de collecter des informations sensibles que leurs propriétaires ont omises de les mettre à l'abri des robots (bots) de Google. Nous utilisons dans cet atelier Google comme un outil de scan. Pour ce faire, il faut tout d'abord maîtriser le langage de recherche de Google pour avoir des résultats pertinents et précis. En effet, Google offre des options de recherches avancées à l'aide d'un ensemble d'opérateurs. Exemples :

"mots recherchés" : Utiliser des guillemets pour rechercher un terme précis ou un groupe de mots.

-requete : Ajouter un signe moins (-) avant un mot ou un nom de site pour exclure tous les résultats qui incluent ce terme. **site** : Permet de restreindre vos recherches à certains sites ou domaines.

info : Permet d'obtenir des informations sur une URL, telles que la version en cache de la page, les pages similaires et les pages qui redirigent vers cette URL.

allintext : Recherche un mot uniquement dans le body d'une page.

intext : même principe, pour les phrases complètes.

allintitle : pour rechercher uniquement dans les titres des pages (balise title).

intitle : même principe, pour rechercher une phrase complète.

allinurl : pour rechercher uniquement dans les URL des pages web.

inurl : même principe, pour rechercher une phrase complète.

Un attaquant a la possibilité de forger des requêtes en utilisant le formalisme adéquat pour récupérer des données privées ou sensibles.

- 1- Trouver la page de login des serveurs de messagerie : **intitle:"Zimbra Web Client Log In"**
- 2- Trouver des mots de passes des serveurs web : **xamppdirpasswd.txt filetype:txt**
- 3- Trouver des mots de passes des serveurs FTP : **inurl:proftpdpasswd**
- 4- Trouver la clé privée d'un serveur web : **intext:"index.of " server.key site:free.fr**
- 5- Accès aux données privées mal protégées : **intext:"index.of " perso site:free.fr**

Pour aller plus loin : <http://www.exploit-db.com/google-dorks/>

B. Quelques exemples de requêtes :

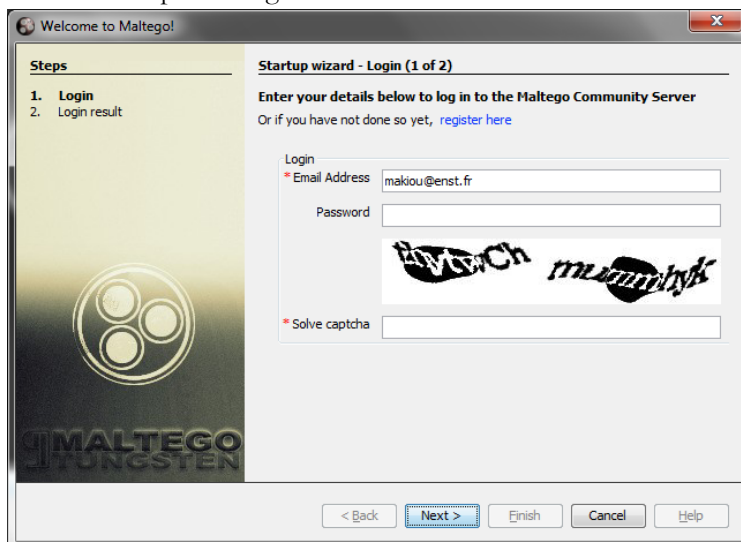
<code>allinurl:/CuteNews/show_archives.php</code> <code>intitle:"Index of" .sh_history</code> <code>intitle:"Index of" .bash_history</code> <code>intitle:"index of" passwd</code> <code>intitle:"index of" people.lst</code> <code>intitle:"index of" pwd.db</code> <code>intitle:"index of" etc/shadow</code> <code>intitle:"index of" spwd</code> <code>intitle:"index of" master.passwd</code> <code>intitle:"index of" httpasswd</code> <code>intitle:"index of" members OR accounts</code> <code>inurl:auth_user_file.txt</code> <code>inurl:orders.txt</code> <code>inurl:"wwwroot/*."</code> <code>inurl:adpassword.txt</code> <code>inurl:webeditor.php</code> <code>inurl:file_upload.php</code> <code>inurl:gov filetype:xls "restricted"</code>	<code>phpinfo.php intext:"index.of"</code> <code>intitle:"index of" user_carts OR user_cart</code> <code>allintitle: sensitive filetype:doc</code> <code>allintitle: restricted filetype:mail</code> <code>allintitle: restricted filetype:doc site:gov</code> <code>inurl:admin filetype:txt</code> <code>inurl:admin filetype:db</code> <code>inurl:admin filetype:cfg</code> <code>inurl:mysql filetype:cfg</code> <code>inurl:passwd filetype:txt</code> <code>inurl:iisadmin</code> <code>Index of /admin</code> <code>Index of /passwd</code> <code>Index of /password</code> <code>Index of /mail</code> <code>"Index of /" +passwd</code> <code>"Index of /" +password.txt</code> <code>index of ftp +.mdb allinurl:/cgi-bin/ +mailto</code>
--	---

C. Maltego

Maltego est un outil de foot printing permettant l'analyse en profondeur des infrastructures telles que les ASs (Autonomous System) ou des éléments d'identification tels que les adresses mail et des comptes de réseaux sociaux (twitter, Facebook).

Pour utiliser Maltego, il faut lancer dans la machine virtuelle (scurité_web_kali), se logger avec le compte root dont le mot de passe est root, puis à partir du menu Applications → récupération d'informations → maltegoce

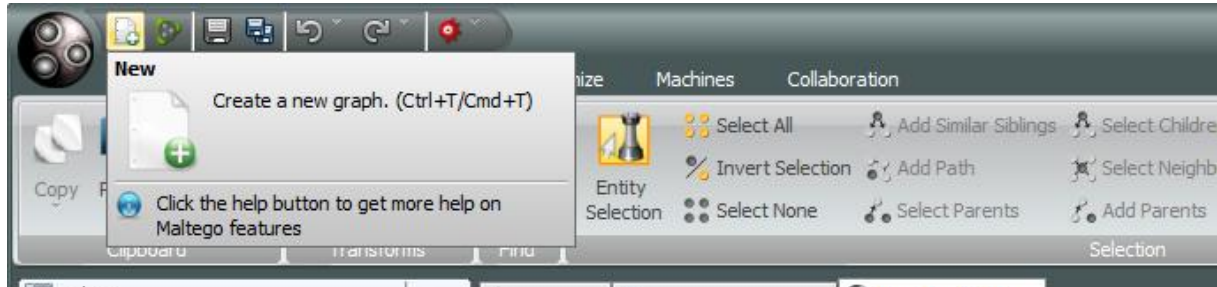
Créer un compte maltego et accéder avec dans l'outil.



Vous pouvez créer un compte pour vous ou utiliser le compte suivant :

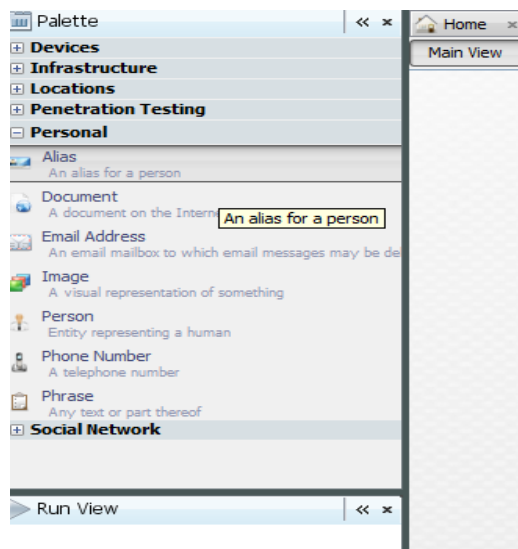
Par la suite, maltego vous propose des templates de scan, nous n'allons pas les utiliser, il faut donc cliquer sur cancel.

Dans le haut du menu principal, nous produisons un nouveau graph de scan comme suit :

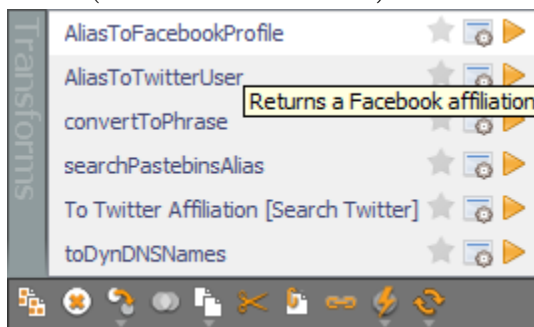


Un exemple de collecte d'informations est le social engineering ; cette approche consiste à collecter le maximum d'informations sur un individu qui possède des accès dans l'entité visée par l'attaque.

Dans la palette des éléments de collecte, on choisit Personal puis Person (un minimum d'informations qu'on possède déjà par le biais de médias ou d'un précédent scan de domaine par exemple).



- 1- Faites glisser l'élément Person dans la zone de graphe :
- 2- Saisissez le nom complet de la personne recherchée
- 3- Procédez à l'analyse de cet élément par un l'ensemble de transformations souhaitées pour cette Person (bouton droit de la souris)



- 4- De la même manière, analyser un domaine (ex.telecom-paristech.fr) et rouvrir des éléments exploitables par les attaquants (serveur de messagerie, serveur DNS, ...)