

Reconnaissance passive

1. Différents outils en ligne de commande

Après avoir effectué des recherches d'informations sur notre cible grâce aux fonctions de Google ou autres. Vous verrez, dans cette partie, les principaux outils de reconnaissance qui permettront de dresser une « architecture réseau » de notre cible (serveur dns, nom des machines, adresse IP etc..). **Il sera important de noter chaque information récoltée.**

Nous voulons récolter des informations sur le domaine « **ntic-center-corporation.com** »

A partir de certaines commandes qui interrogent des serveurs de bases de données, on peut soutirer des informations importantes pour la phase d'exploitation, comme des adresses IP, les serveurs de messagerie, des sous domaines etc...

Cette démarche permet d'obtenir des informations sur la cible, diffusées publiquement, mais pouvant être confidentielles (diffusées généralement par erreur ou insouciance).

1.1 Outils de reconnaissance

The Harvester

Pendant la phase de reconnaissance, l'outil The Harvester se révélera très utile. Il s'agit d'un simple script Python très efficace. Il permet de cataloguer rapidement et précisément les adresses de courriers électroniques et les sous-domaines directement liés à la cible.

Il est important de toujours utiliser la dernière version de The Harvester, car de nombreux moteurs de recherche actualisent et modifient régulièrement leurs systèmes.

Pour exécuter The Harvester entrez la commande :

theHarvester -d ntic-center-corporation.com -l 10 -b google

L'option **-d** permet de préciser le domaine cible.

L'option **-l** permet de limiter le nombre de résultats renvoyés. Dans notre exemple, nous demandons à l'outil de renvoyer uniquement dix résultats.

L'option **-b** précise le répertoire public dans lequel se fait la recherche. Nous avons plusieurs choix, notamment Google, Bing, PGP, LinkedIn. Si vous n'êtes pas certain de la source de données à employer, l'option **-b all** permet d'effectuer la recherche dans tous les référentiels reconnus.

Whois

Pour recueillir des informations supplémentaires sur une cible, une solution très simple, mais efficace, consiste à employer Whois. Ce service permet d'accéder à des informations précises sur la cible, notamment les adresses IP ou les noms d'hôtes des serveurs DNS de la société.

Exécutez cette commande :

whois ntic-center-corporation.com

```
Registry Registrant ID:  
Registrant Name: Zokou osso paul  
Registrant Organization:  
Registrant Street: 1 square chalgrin  
Registrant City: asnieres sur seine  
Registrant State/Province:  
Registrant Postal Code: 92600  
Registrant Country: FR  
Registrant Phone: +33.665514291  
Registrant Phone Ext:  
Registrant Fax: +33.981098070  
Registrant Fax Ext:  
Registrant Email: paul_zokou@yahoo.fr  
Registry Admin ID:  
Admin Name: ntic center corporation  
Admin Organization: ntic center corporation
```

Il est important de conserver ces informations et de prêter une attention particulière au Name Server.

La recherche whois est également possible avec un navigateur web, <http://www.whois.net> il faut indiquer la cible dans le champ de saisie.



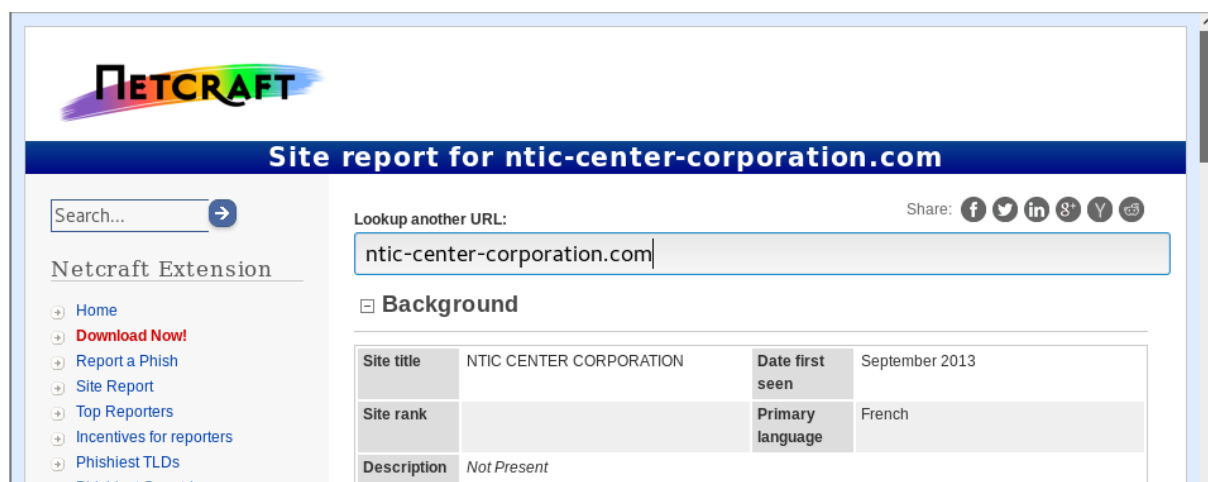
Your Domain Starting Place...

A screenshot of the Whois.net search interface. It shows a light grey rectangular box with rounded corners. Inside the box is a white search input field containing the text "ntic-center-corporation.com". To the right of the input field is a green square button with a white magnifying glass icon.

Examinez attentivement les informations présentées. Il se peut qu'il y ait des informations supplémentaires par l'interface web ou le contraire.

Netcraft

Netcraft constitue une autre excellente source d'informations. Son site est accessible à l'adresse http://toolbar.netcraft.com/site_report



Site report for **ntic-center-corporation.com**

Search... →

Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries

Lookup another URL:

Share: [f](#) [t](#) [in](#) [g+](#) [Y](#) [v](#)

☐ Background

Site title	NTIC CENTER CORPORATION	Date first seen	September 2013
Site rank		Primary language	French
Description	Not Present		

Netcraft renvoie tous les sites web qu'il connaît qui comprennent les mots recherchés. On peut ensuite cliquer dans la colonne « Site Report ». Le rapport qui s'affiche fournit de nombreuses informations sur le site (l'OS, le service web, le DNS etc...). Si vous récupérez des informations qui vous ont échappées aux recherches précédentes, ajouter les à la liste de cible.

Host

Très souvent, les actions de reconnaissance produiront non pas des adresses IP, mais des noms d'hôtes. Lorsque c'est le cas, la commande host se chargera d'en faire la traduction à notre place.

Nos recherches précédentes (whois et netcraft) nous ont amenées à découvrir 1 serveur DNS. Pour convertir le nom en adresse IP, utilisez la commande Host :

```
root@kali: ~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
root@kali:~# host dns200.anycast.me  
dns200.anycast.me has address 46.105.206.200  
root@kali:~#  
root@kali:~#
```

host *leserveurdns*

Ce qui vous donnera leur adresse IP.

Que faire une fois qu'on dispose de l'adresse IP du DNS ?

Les serveurs DNS sont des cibles de choix pour les hackers et les testeurs d'intrusion, car ils contiennent généralement des informations de forte valeur. Les serveurs DNS conservent des enregistrements qui mettent en correspondance l'adresse IP et le nom d'hôte pour tous les appareils qu'ils connaissent.

1.2 Outils d'extraction DNS

Nslookup

Le premier outil que nous utiliserons pour exploiter le DNS se nomme NSLookup. Il permet d'interroger les serveurs DNS et d'obtenir des enregistrements sur les différents hôtes qu'ils connaissent.

NSLookup peut opérer en mode interactif. Autrement dit, vous lancez le programme puis vous saisissez les différentes commandes pour le faire fonctionner correctement. Ouvrez une fenêtre de terminal et exécutez la commande suivante :

Nslookup

L'invite du système d'exploitation, en général #, est alors remplacée par >, qui correspond à l'invite de l'outil. Nous pouvons alors saisir les informations supplémentaires nécessaires au fonctionnement de NSLookup.

On commencera par ajouter la syntaxe server "ip_du_DNS", remplacer l'ip_du_dns par l'adresse extraite par la commande host.

>server l'@ip

```
root@kali:~# nslookup
> server 46.105.206.200
Default server: 46.105.206.200
Address: 46.105.206.200#53
>
```

Nslookup accepte la commande et réaffiche une invite de commande. Nous précisons ensuite le type d'enregistrement qui nous intéresse. Pendant la phase de reconnaissance, plusieurs types d'enregistrements pourront nous fournir des informations intéressantes. Pour connaître l'intégralité de la liste de tous ces types, avec leur description, n'hésitez pas à exploiter vos nouvelles compétences Google. Si nous voulons des informations générales, nous fixons le type à any, mais dans notre cas on recherche l'@ du ou des serveurs de messagerie de ntic-center-corporation. On fixe donc le type à MX :

>set type =mx

Ensuite il vous renvoie sur une invite de commande où il suffira de mettre le domaine ciblé, dans notre cas ntic-center-corporation.com

> **ntic-center-corporation.com**

```
> set type=mx
> ntic-center-corporation.com
Server:      46.105.206.200
Address:     46.105.206.200#53

ntic-center-corporation.com      mail exchanger = 5 mx2.ovh.net.
ntic-center-corporation.com      mail exchanger = 1 mx1.ovh.net.
ntic-center-corporation.com      mail exchanger = 100 mxb.ovh.net.
```

Et une liste des différents enregistrements sera affichée.

Nslookup nous donnera comme réponse, le (ou les) nom de la machine qui pointe sur l'enregistrement demandé, en l'occurrence le serveur de messagerie, et pour connaître son IP il suffit de faire à nouveau la commande host sur ce nom.

Il est aussi possible de récolter des informations sans posséder l'adresse du serveur DNS, juste à partir du nom de domaine.



Pour extraire des informations du DNS, Dig se révèle aussi un outil particulièrement approprié.

dig ntic-center-corporation.com

```
root@kali:~# dig ntic-center-corporation.com

; <<>> DiG 9.10.3-P4-Debian <<>> ntic-center-corporation.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7567
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;ntic-center-corporation.com.      IN      A
```

Il va interroger les serveurs DNS à la recherche d'informations sur le domaine ntic-center-corporation.com. Dans notre exemple ci-dessus, le serveur retourne seulement un enregistrement car il n'y a pas de type précisé. Pour préciser l'enregistrement recherché :

#**dig ntic-center-corporation.com any @8.8.8.8**

```
;; ANSWER SECTION:
ntic-center-corporation.com. 5 IN      TXT      "v=spf1 include:mx.ovh.com ~all"
ntic-center-corporation.com. 5 IN      MX        1 mx1.ovh.net.
ntic-center-corporation.com. 5 IN      MX        5 mx2.ovh.net.
ntic-center-corporation.com. 5 IN      MX        100 mxb.ovh.net.
ntic-center-corporation.com. 5 IN      SOA       dns200.anycast.me. tech.ovh.net. 2017042600
3600 3600000 300
ntic-center-corporation.com. 5 IN      A         45.58.142.8
```

Grâce à cette recherche on va récupérer les enregistrements, cette image nous permet de récupérer une information importante. Les serveurs de noms, de messagerie mais aussi de **savoir que le dns200.anycast.me est le serveur de nom faisant autorité.**

Ce qui veut dire que le serveur dns200.anycast.me possède tous les enregistrements qui sont ensuite transférés sur les dns secondaires. On appelle cela le transfert de zone. Sur les DNS mal sécurisés, il est donc possible d'extraire toutes les informations confidentielles des enregistrements DNS, en essayant d'effectuer un transfert de zone sur le serveur qui fait autorité.

Nous avons précédemment récupéré son IP : 46.105.206.200

Exécutez cette commande :

dig « @ip du SOA » ntic-center-corporation.com axfr

Dans notre cas la requête sera refusée, mais dans de nombreux cas les serveurs DNS sont mal configurés et vont le permettre.

```
root@kali:~# dig 46.105.206.200 ntic-center-corporation.com axfr

; <<>> DiG 9.10.3-P4-Debian <<>> 46.105.206.200 ntic-center-corporation.com axfr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35045
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 1280
;; QUESTION SECTION:
;46.105.206.200.                IN      A

;; ANSWER SECTION:
46.105.206.200.                5       IN      A      46.105.206.200

;; Query time: 2006 msec
;; SERVER: 192.168.99.2#53(192.168.99.2)
;; WHEN: Thu Dec 14 15:18:03 CET 2017
;; MSG SIZE rcvd: 59

; Transfer failed.
```

Dnsenum

Dnsenum est aussi un outil permettant l'extraction de données DNS à partir d'un nom de domaine. Cependant, il permet aussi de faire du Brute Forcing sur les serveurs de noms, afin de soutirer de nombreuses informations supplémentaires comme les enregistrements confidentiels, les plages IP et les adresses d'exclusion. Pour cela, il lance des recherches à partir d'un fichier qui contient de nombreux mots (généralement des noms de machines utilisés régulièrement) en y rajoutant la cible et, si cela donne une recherche positive, cela signifie que l'enregistrement existe. Mais pour faire cela, une grande quantité de requêtes est faite auprès du DNS, ce qui peut alerter les administrateurs. Pour utiliser dnsenum la commande est la suivante :

dnsenum ntic-center-corporation.com

Il va donc donner les enregistrements trouvés et aussi essayer de faire un transfert de zone sur les serveurs de noms trouvés.

1.3 Les métadonnées

Les métadonnées sont souvent définies comme “des données à propos des données”. Lorsqu’un utilisateur crée un document, des données supplémentaires sont générées et enregistrées avec le fichier. Elles comprennent différents éléments d’information comme :

- Nom du fichier
- Sa taille
- Son propriétaire
- L’emplacement

Cela peut donc donner des noms d’utilisateurs, des chemins réseaux, des noms d’ordinateurs etc...

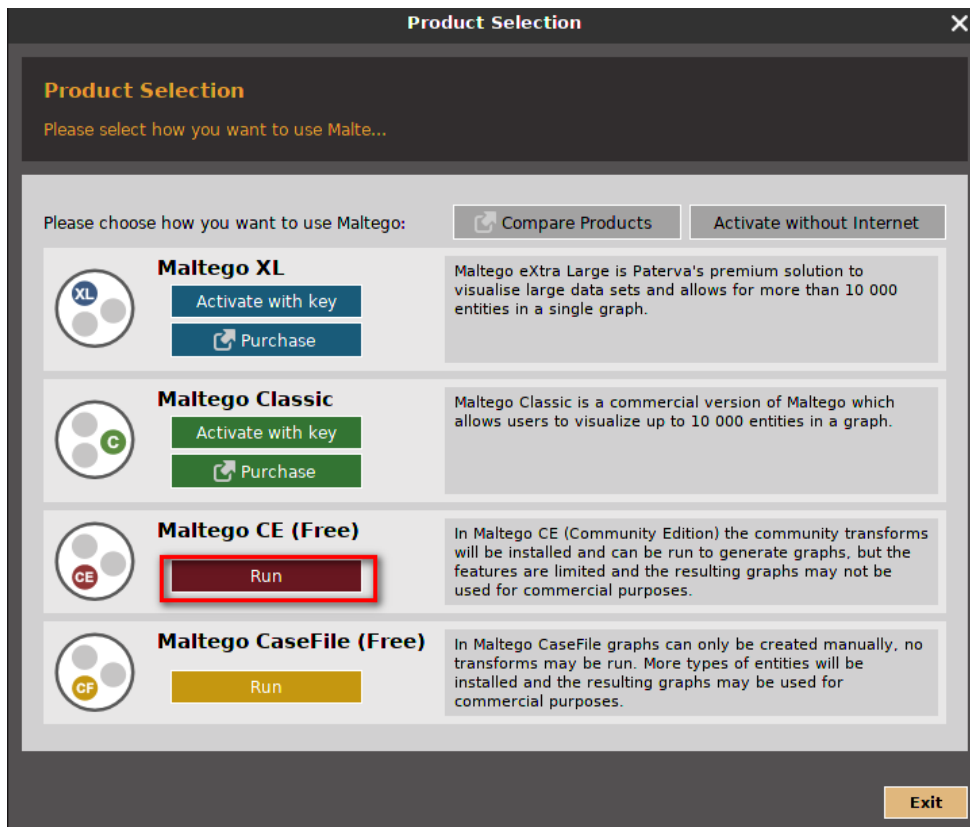
2. Le tout-en-un graphique

Ce logiciel Open-source permet de grouper la totalité des commandes vues précédemment et tout cela en interface graphique. Ce qui nous permet donc de dresser une architecture, mais aussi peut-être de trouver des informations qui auraient pu nous échapper.

Pour utiliser Maltego vous aurez besoin de faire une inscription gratuite, il existe aussi une version payante plus complète. Pour lancer Maltego, exécutez cette commande dans le terminal :

maltego

Une fois l’application lancée, cette fenêtre apparaît :



Choisir la version « CE free »

Configure Maltego

STEPS

1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Privacy Mode Options
7. Ready

LICENSE AGREEMENT: Please read and accept the following License Agreement.

**General Terms and Conditions
for Software License Agreements of Paterva**

(Effective 23 July 2018)

These General Terms and Conditions apply to all licenses (hereinafter referred to as "**Software Licenses**") which are issued by Paterva (Pty) Ltd. (incorporated in South Africa under registration number 2008/005705/07), (hereinafter referred to as "**Licensor**") to its customers (hereinafter referred to as "**Licensee**") (Licensor and Licensee also referred to as "**Party**" and collectively the "**Parties**"), and which refer to the client components "Maltego XL", "Maltego Classic", "Maltego CE", "Casefile" ("**Client Components**") or the server components "private CTAS", "ITDS", "Comms Server", "MDS" ("**Server Components**") (Client Components and Server Components as well as other computer programs provided by the Licensor hereinafter also referred to as "**Software**"). Software subject to these General Terms and Conditions is the intellectual property of the Licensor and/or Maltego Technologies GmbH, registered in the district court Munich, Germany under no. HRB 236523 ("**Maltego**"). To the extent that Software is owned by Maltego, the Licensor has sufficient rights to license same to the Licensee.

1. Contractual Object

1.1. These General Terms and Conditions govern the Software Licenses issued to the Licensee by the Licensor by way of a **Software License Agreement**. Sec. 3 specifies the scope of each Software License subscribed regarding the specific Software being licensed as well as the content, location, time and extent of the user rights.

1 ☒ Accept

2

Cliquez sur « Next ».

Welcome to Maltego!

STEPS

1. Welcome
2. Login
3. Login result
4. Select Transform Seeds
5. Install Transforms


LOGIN:

Enter your details below to log in to the Maltego Community Server
Or if you have not done so yet, [register here](#)

Login

* **Email Address**

Password



* **Solve captcha**

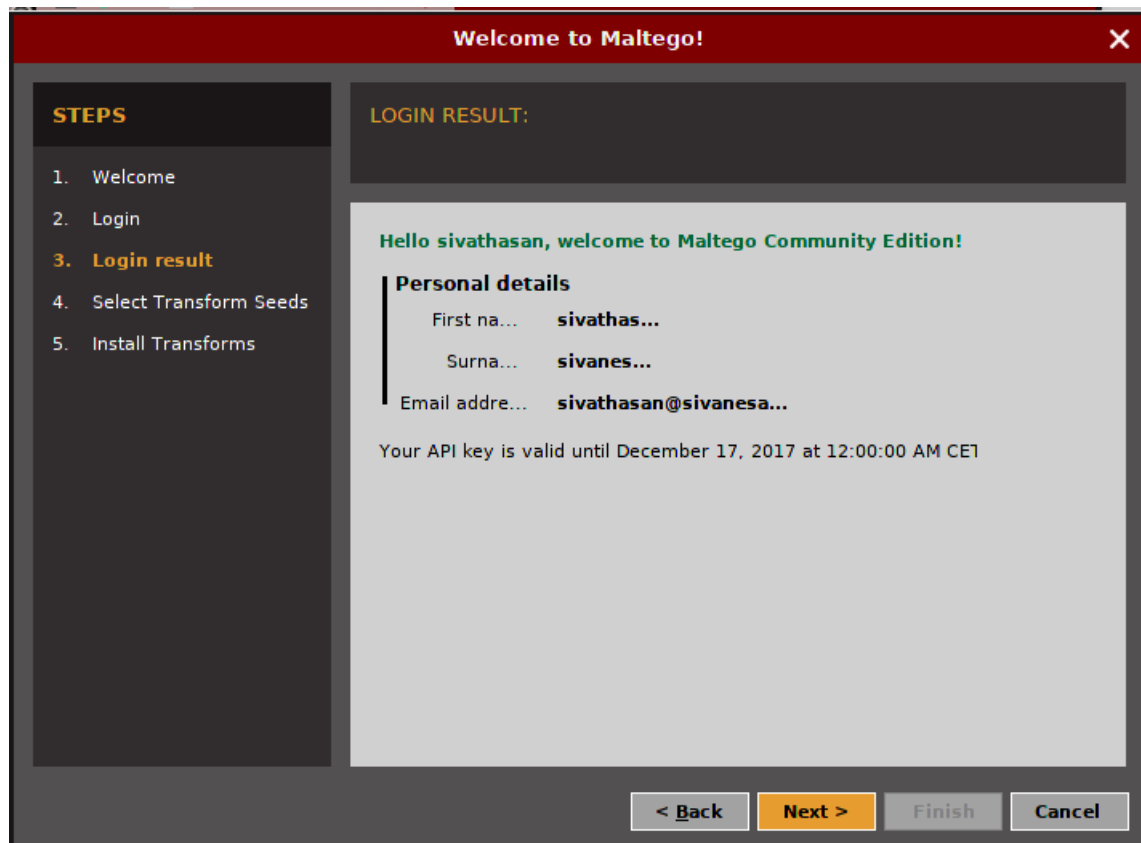
Il faut vous créer un compte, pour ce faire cliquez sur « Register here ».

Ce qui vous envoie sur le site de Maltego pour vous créer un compte. Une fois l'inscription faite, allez dans votre boîte mail et acceptez la création.

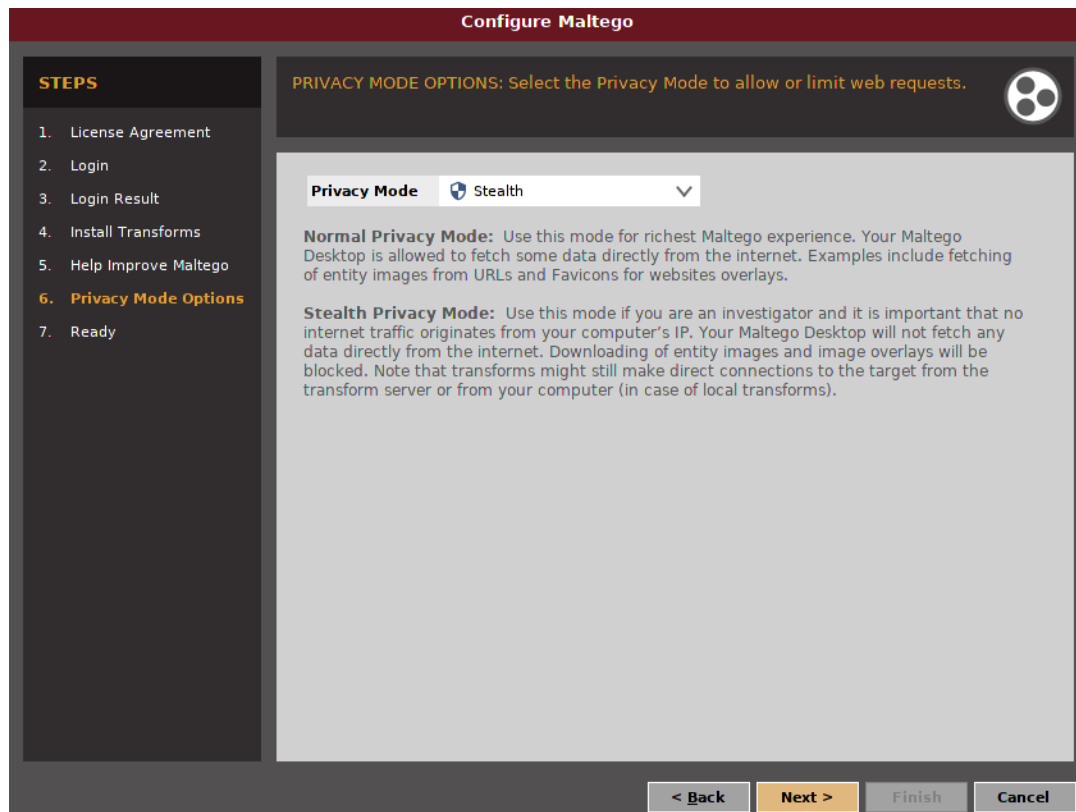
Si vous ne souhaitez pas utiliser votre compte mail vous pouvez utiliser un mail temporaire :

<https://10minutemail.net/?lang=fr>

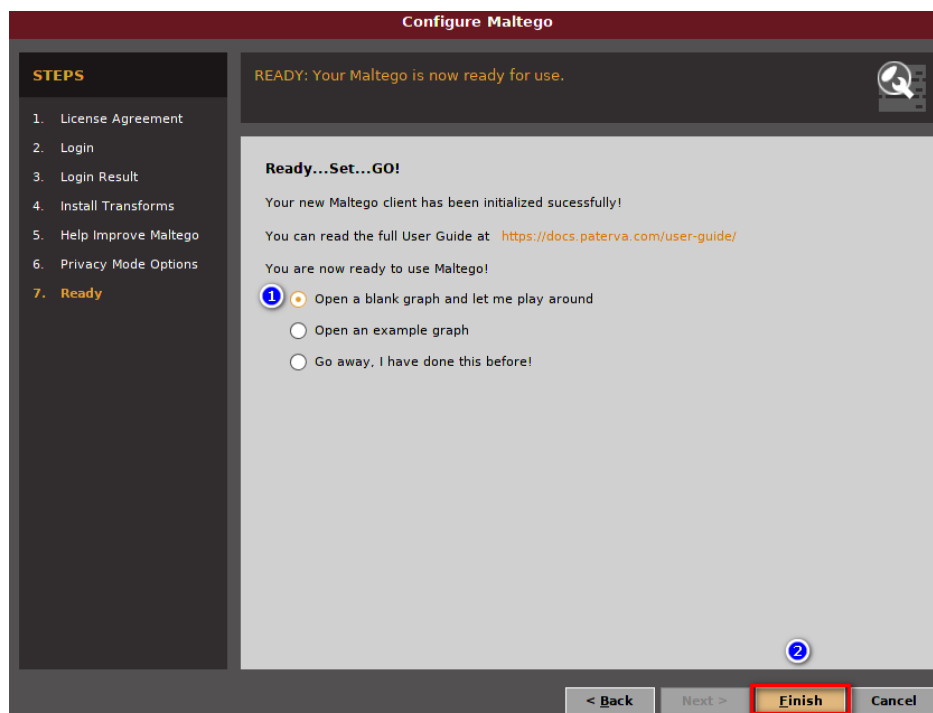
Une fois le code obtenu vous serez connecté.



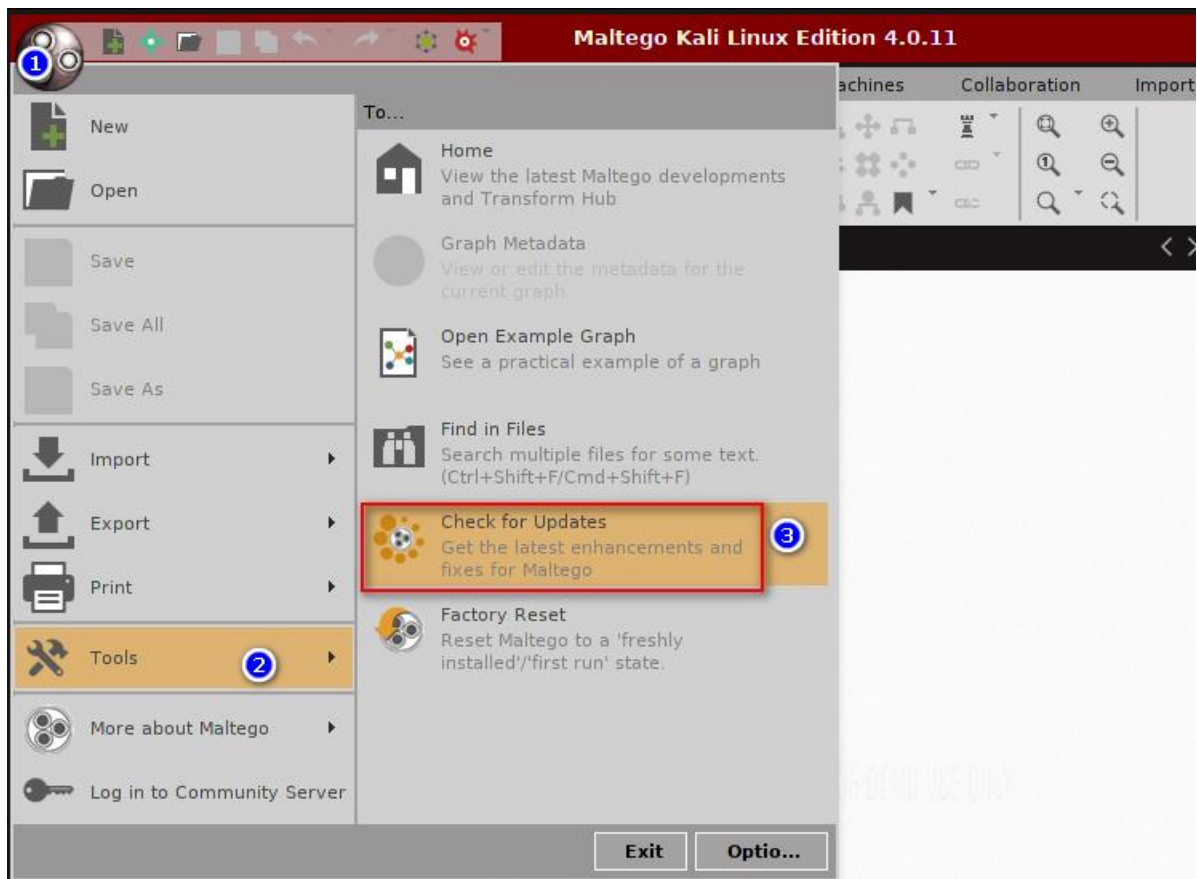
Utilisez le mode Stealth et cliquez sur « Next ».



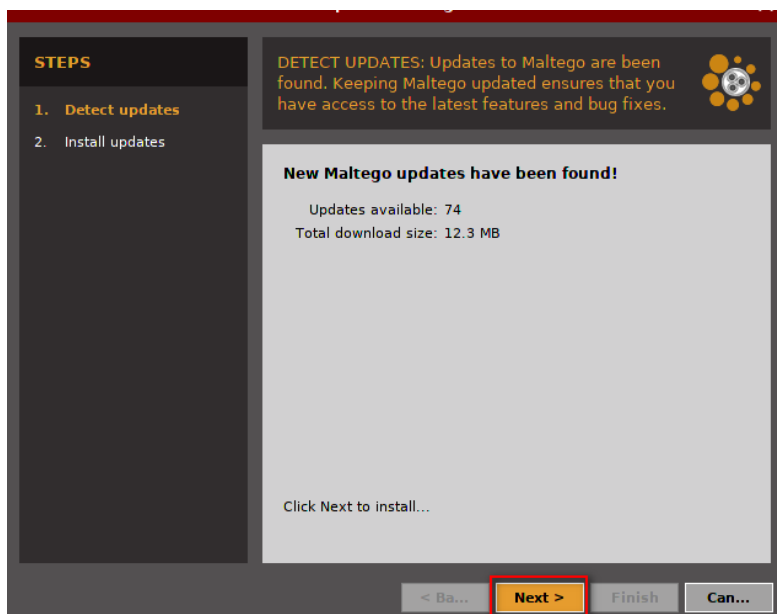
Des mises à jour seront effectuées. Sélectionnez “Open a blank graph and let me play around” et “Finish”.



Mise à jour:

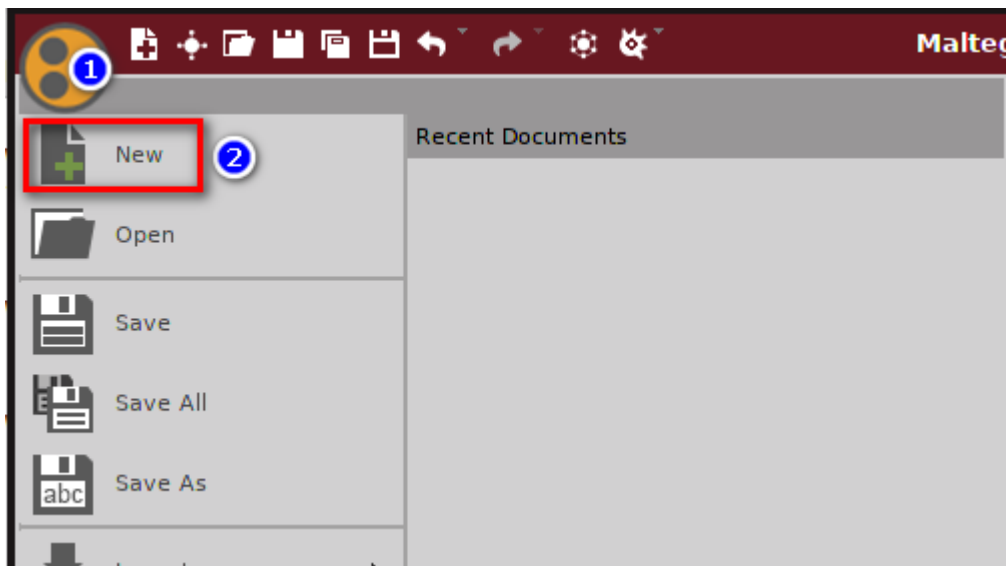


Cliquer sur Next pour mettre a jour Maltego

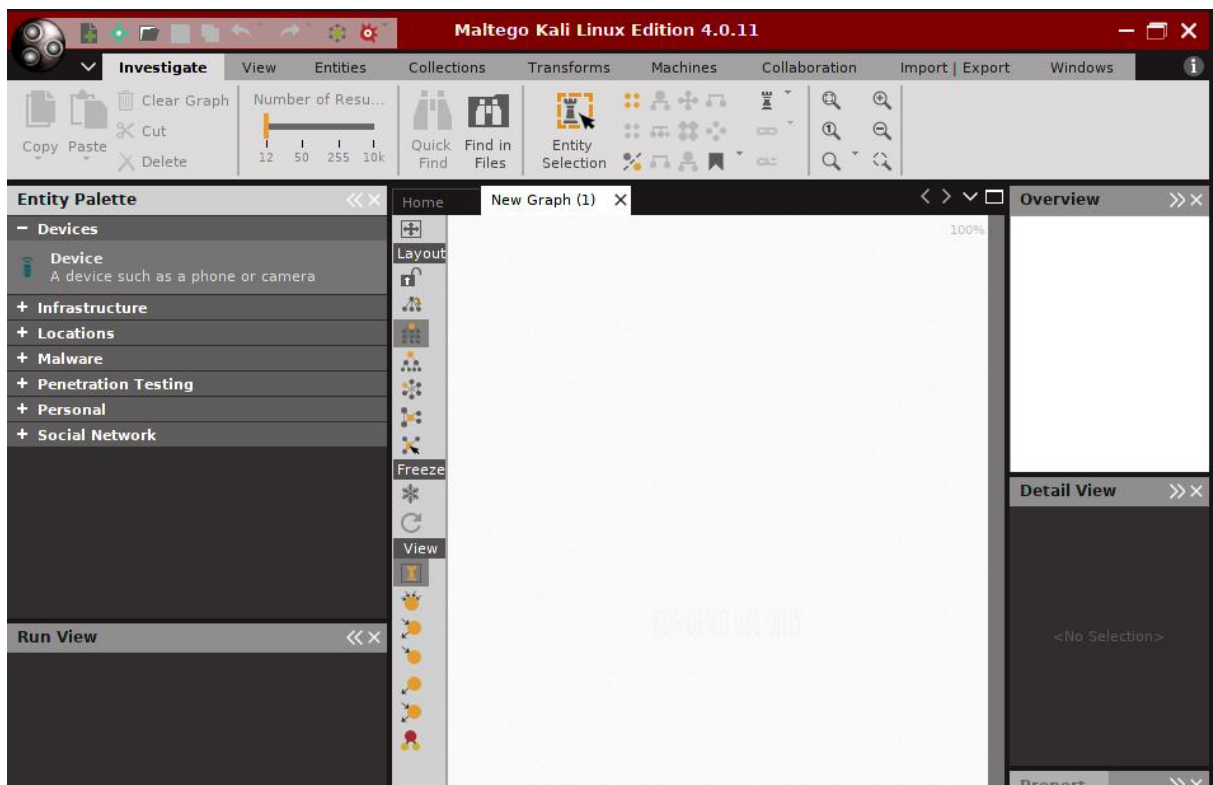


Cliquer sur "restart" a la fin pour relancer MaltegoCE

Démarrer un investigation:



Présentation du logiciel :



Sur le côté gauche on y voit Palette avec plusieurs onglets :

Devices : Correspond aux caméras et Téléphone

Infrastructure : Tout ce qui est serveur DNS, Serveur de messagerie, Adresse IP, Site web etc...

Locations : Lieu où est située l'infrastructure

Malware : Base de données de Malware connue avec leur Hashs.

Penetration Testing :

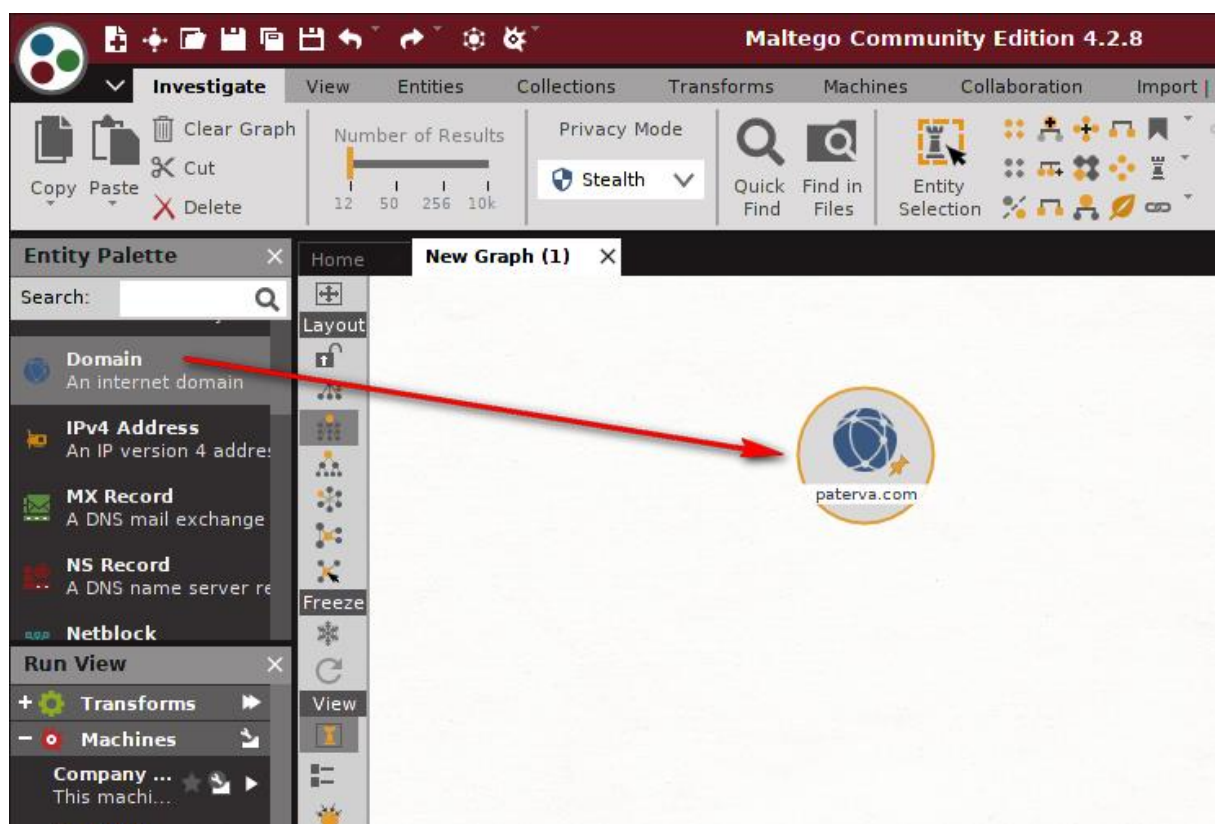
Personal : Documentation, E-mail, n° de téléphone etc...

Social network : Compte facebook , twitter etc...

Toutes ces informations permettent de dresser une architecture complète de la cible.

Mise en pratique :

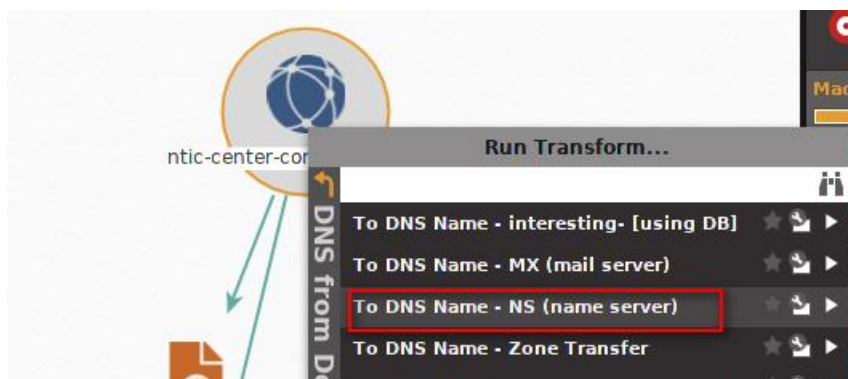
Créer un Domain :



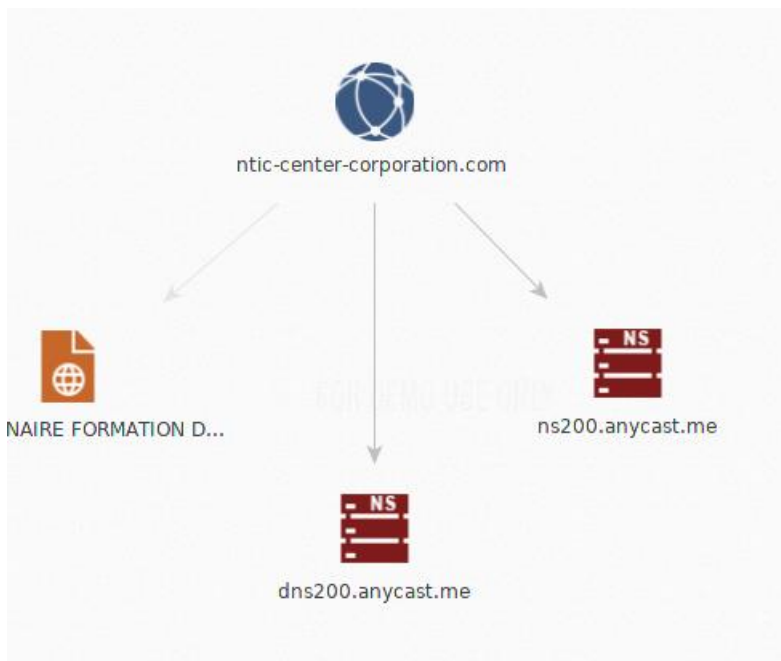
Renommer le domaine en nticcc :



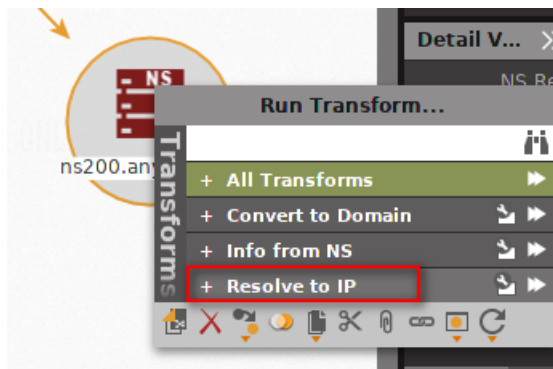
On veut ensuite extraire les serveurs DNS de **ntic-center-corporation.com**, pour ce faire faites un clic droit sur ntic-center-corporation.com « Run transform » ➔ « DNS from domain » ➔ « To DNS name – NS »



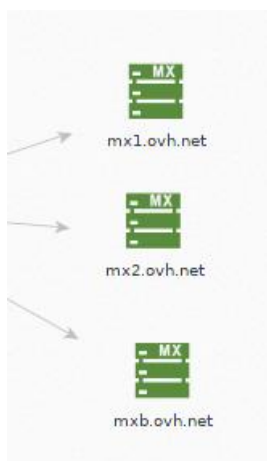
Ce qui permettra à Maltego d'extraire des informations sur les serveurs de noms du domaine ntic-center-corporation.com. Voilà que deux nouvelles entités apparaissent qui correspondent aux 2 serveurs de nom vus précédemment.



On veut ensuite soustraire l'@ip de ns200.anycast.me. Pour cela faire un clic droit dessus ➔ « Resolve to ip » ➔ « To IP Address ». Maltego effectue en tâche de fond la commande host sur le nom de machine et affiche son @ip.



On souhaite récupérer les serveurs de messageries appartenant à ntic-center-corporation.com. Pour ce faire, faites un clic droit sur ntic-center-corporation.com ➔ « DNS from Domain » ➔ « To DNS Name – MX ». Ce qui en tâche de fond fera une requête DNS sur les enregistrements MX.



On veut aussi récupérer des @ e-mail appartenant à ntic-center-corporation.com. On fait donc un clic droit sur ntic-center-corporation.com ➔ « E-mail Adresses from domain » ➔ « to Emails@domain ».

Ce qui nous donne aucun résultat alors qu'avec la méthode en ligne de commande nous avons obtenu une adresse mail

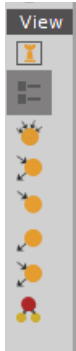
.

Il est possible de dresser votre graphique comme bon vous semble en déplaçant les entités avec la souris, il est aussi possible de le mettre sous différentes positions et vues.

Pour les modifier, cliquez sur les boutons situés sur le côté droit, pour voir les différentes topologies.



Il est aussi possible de changer la vue en cliquant sur un des trois boutons différents :



Ceci est une petite présentation de la puissance de l'outil Maltego, mais grâce à vos nouvelles compétences google n'hésitez pas à rechercher de la documentation.

Mise en pratique :

Effectuez une recherche complète sur un domaine de votre choix et dressez son architecture sur Maltego.