Devoir 1

Exercice 1 :

Question :

Explorez les sites Web de Maltego et Shodan pour comprendre leurs capacités. Notez comment Maltego permet de visualiser les réseaux et les connexions, tandis que Shodan est utilisé pour rechercher des informations sur les appareils connectés à Internet.

Sont : La Cybersécurité, une enquête criminelle, de la veille Concurrentielle, l’évaluation des menaces possible ou même pour la cybersécurité. À l'aide de son interface GUI il présente un Exercices 2 :

Question :

En utilisant ces deux outils, faites une analyse de vulnérabilités du site Web https://uqo.ca/. Vous devez écrire un rapport en structurant toutes les informations que vous aviez collectées.

Solution :

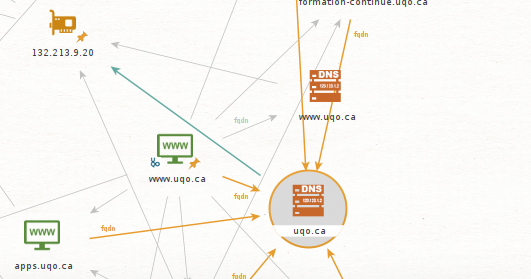
1. Récapitulatif détaillé des activités réalisées

* Collecte des données sur le site www.uqo.ca (domaines, sous-domaines, adresses ip associées aux domaines, relations entre les entités et les liens internes et externes) : Grâce à maltego nous avons pu déterminer le principale domaine (uqo.ca avec pour adresse ip 132.213.9.20) ;

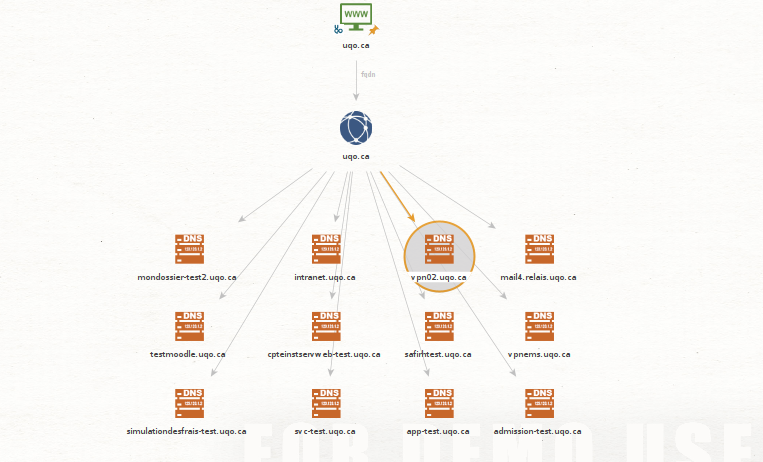
Solution :

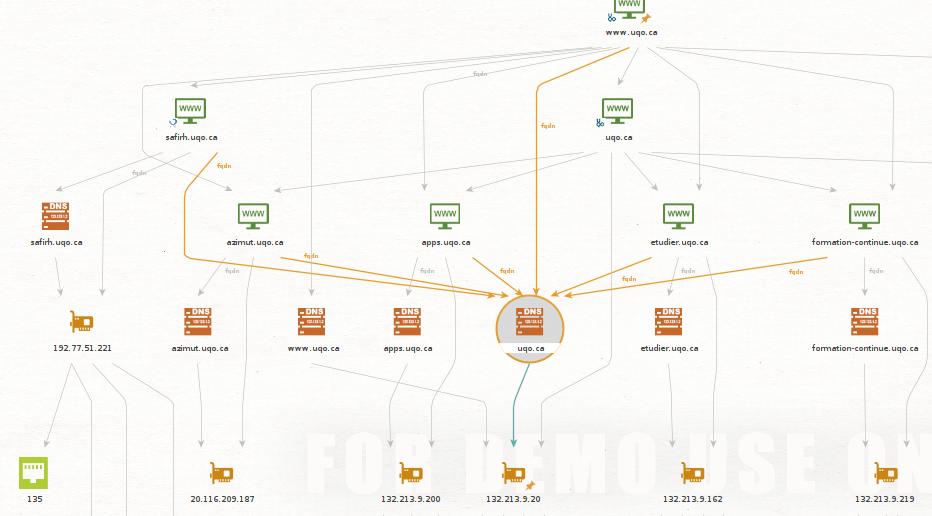
Maltego est un logiciel de OSINT qui permet de ressortir un graphe montrant des liens entre des entités immatérielles et matériels dans un réseaux. Pour établir ses liens, il fait une cueillette d’informations à partir de plusieurs sources publiques sur internet (réseaux sociaux, sites internet, base de données) a l’aide la notion de « transformation, qui sont des scripts prédéfinis ou personnalisés qui extraient, manipulent et enrichissent les informations » dont les objectifs diagramme à l’utilisateur qui raffinera à sa convenance.

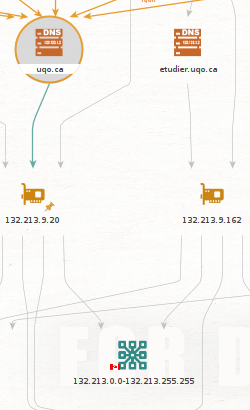
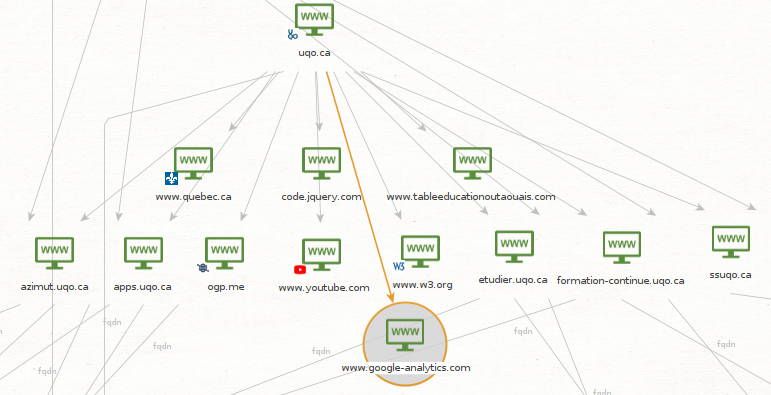
Shodan est un site internet qui permet de retrouver les machines, routeurs, imprimantes, serveurs visibles sur le réseau internet ; Elle référence également tous les résultats des ports ayant été balayés sur le réseau internet. On peut appliquer des filtres tel que (par pays, par ville, par types d’équipements réseaux… etc.) pour avoir des informations plus spécifiques. Elle possède deux interfaces à savoir une interface GUI et ligne de commande. Shodan a pour objectifs de fournir une image complète d’internet par le biais des sites web qui sont hébergés sur des appareils. Pour le faire, shodan collecte de l’unités de données fondamentale un objet appelle bannières, où sont stockées les informations des services.



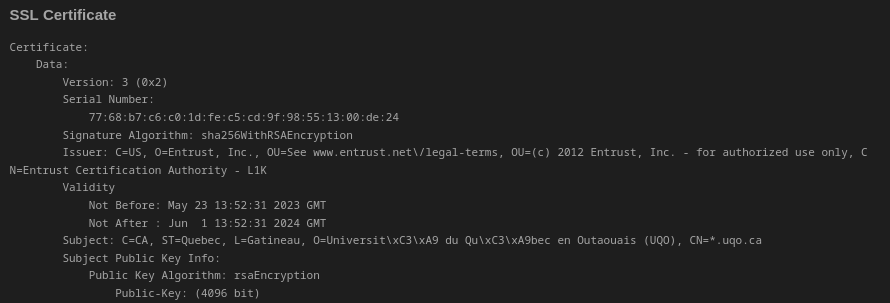
Par la suite nous avons obtenu les noms de sous-domaines, leurs adresse ip respectives et bla plage d’adresses ip du reseau de DNS (etudier.uqo.ca, apps.uqo.ca, safirh.uqo.ca …etc.) ;



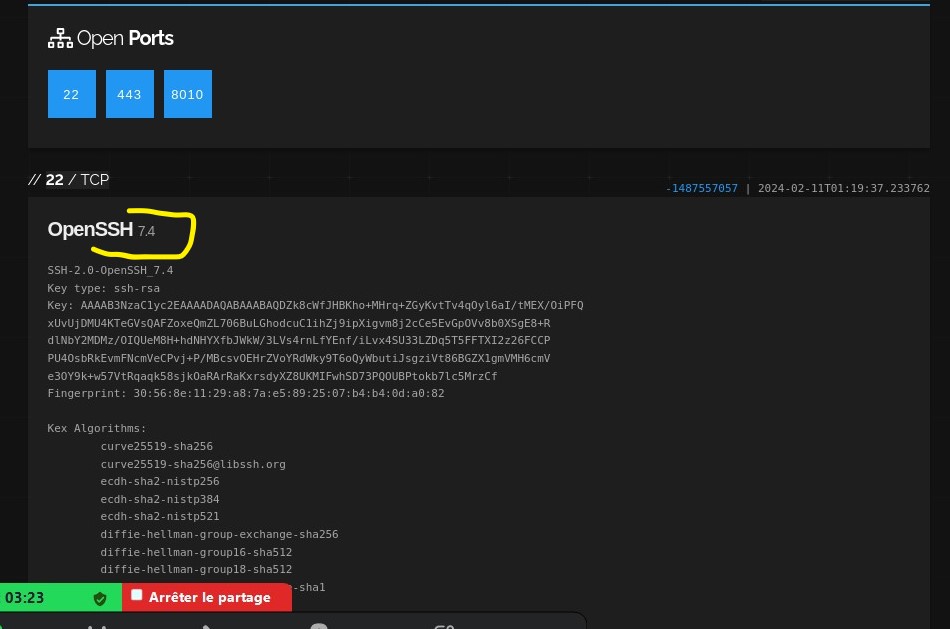


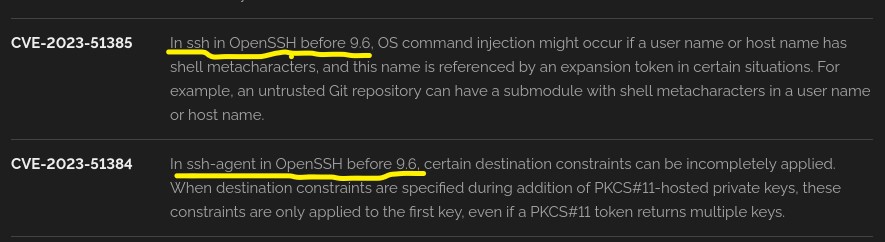
Enfin, toujours grâce à maltego nous avons obtenu les relations entre les entités, les liens internes et externes du site. 

* Recherche de la présence du type de sceau de confiance du site web. Pour le faire nous avons introduit dans la barre de recherche dans shodan le nom de domain « uqo.ca » et nous avons constaté que [www.uqo.ca](http://www.uqo.ca) utilise Entrust, Inc version 3.

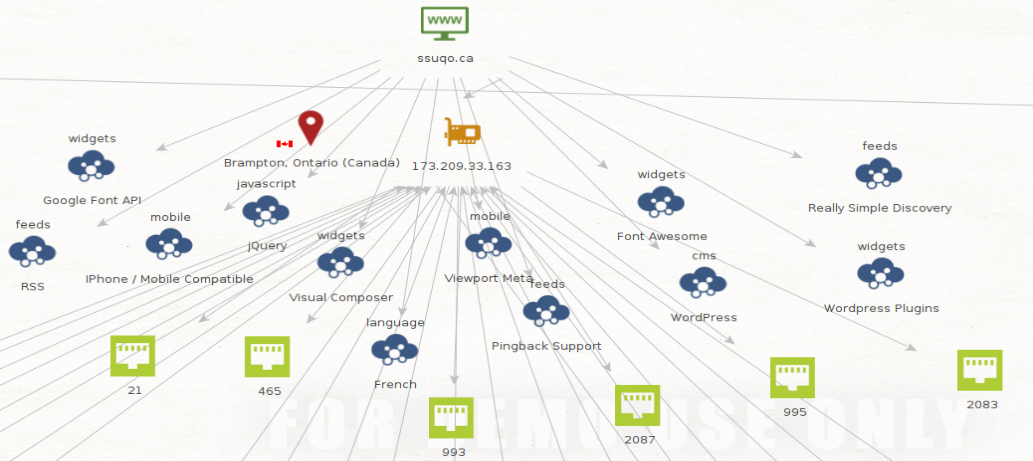


* Localiser les serveurs web et autres (NGINS, APACHE…) en lancant une recherche sur les adresses ip des noms de domaines sur shodan on a pu déterminer les serveurs SMTP, FTP et les serveurs web ngins, apache ayant pour adresses respectives (132.213.9.20 et 132.213.9.106).
* Vérifications des paramètres des serveurs web (certificats SSL, ports ouverts et configuration de sécurité). Grâce à maltego et shodan les principaux ports toujours ouverts sont les ports 80, 443, 8443, 8010 et 21, 25, 26, 993, 2082, 2083, 2086, 2087, 2095 sur l’adresse ip 173.209.33.163
* Recherches de vulnérabilités dans le système de gestion de contenus et des plugins : principalement sur le serveur nginx et Apache avec pour adresses ip 132.213.9.20, 132.213.9.106. Après avoir introduit ses adresses ip dans la barre de recherche de Shodan, on peut conclure que l’adresse 132.213.9.20 ne présente aucune vulnérabilité. Cependant, on observe des vulnérabilités sur l’adresse 132.213.9.106 l’adresse de [www.uqo.ca](http://www.uqo.ca). il s’agit des CVE-2023-51385, CVE-2023-51384 et CVE-2023-48795 qui se rapportent aux versions antérieures de OpenSSH 9.6. La version utilisée par le site de l’Uqo étant de 7.4 d’où sujette à une vulnérabilité selon <https://nvd.nist.gov/vuln/detail/CVE-2023-51385>, <https://nvd.nist.gov/vuln/detail/CVE-2023-51384> et https://nvd.nist.gov/vuln/detail/CVE-2023-48795.



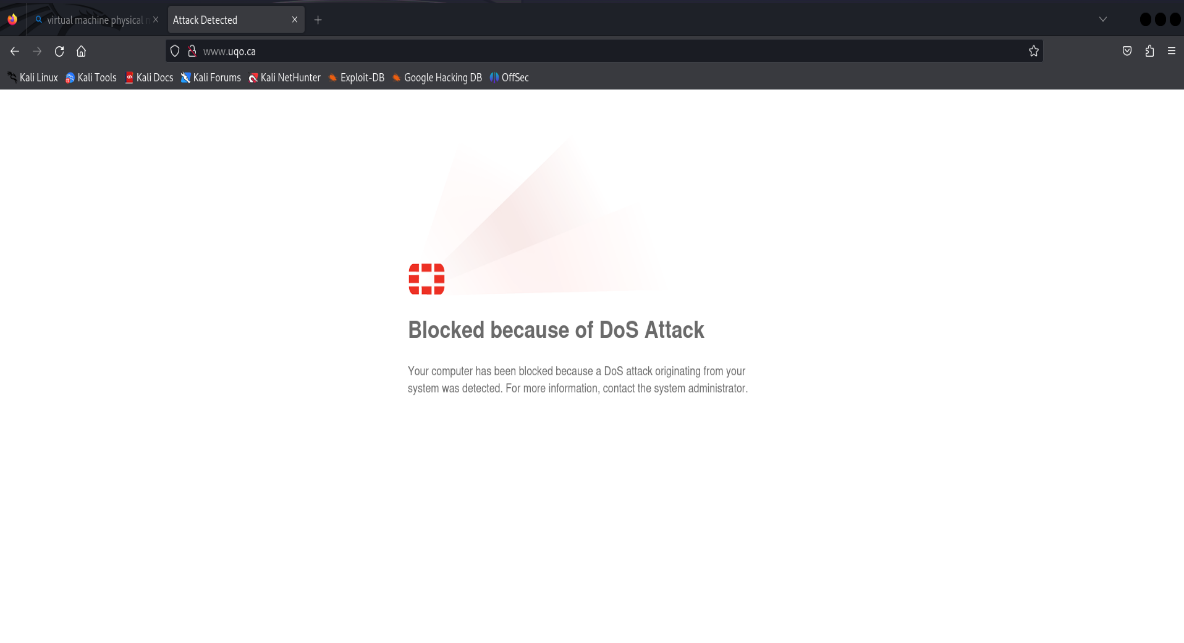


le site de la clinique [www.ssuqo.ca](http://www.ssuqo.ca) n’a pas de sceau SSL ; Tel que présente la transformation web technologies de maltego. Mais une de nos machines, parvient à accéder au site de la clinique avec le sceau de confiance SSL; [https://ssuqo.ca](https://ssuqo.caa/).



On a fait une attaque DDos au niveau de la couche de transport en lançant un scan de ports de three handshake sur l’adresse réseau des serveurs DNS du site de l’uqo 132.213.0.0/16 après un peu plus d’une heure mon adresses ip a été détecté comme source d’attaque DDos.



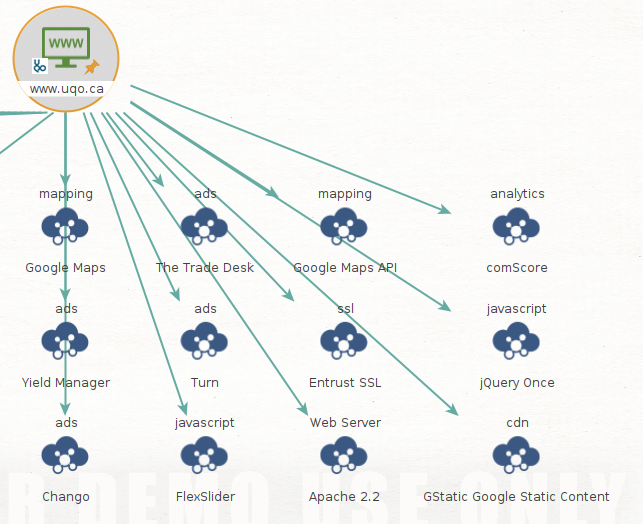


* Recherches des fichiers robots.txt et sitemap.xml pour avoir les informations sur la structure du site et les pages autorisées ou exclues.

La recherche des fichiers robots.txt et sitemap.xml pour avoir les informations sur la structure du site et les pages autorisées ou exclues a été sans réussite.

1. **Analyse de l’impact de l’activité :**

A travers la collecte des données effectuées on a pu retracer le parcours d’une requête https de mon navigateur jusqu’au serveur web. Pour ce fait, on a obtenu des adresses ip des noms de domaine, les deuxièmes niveaux de domaine, on les a localisés géographiques avec les serveurs et les ports ouvert et les technologies utilisés pour concevoir le site web [www.uqo.ca](http://www.uqo.ca), cela malgré la présence du VPN Fortinet d’adresse ip 132.213.238.224 ; Ainsi tout attaquant pourrait recueillir toutes ses informations et les affiner son attaque à une technologie spécifique tel qu’au serveur web Apache de version 2.4.6 utilisé par le site de UQO. Grâce à toutes ses informations on a pu identifier une absence de sceau de sécurité dans la communication entre notre navigateur et la page [www.ssuqo.ca](http://www.ssuqo.ca). Car les messages entre les clients et lui ne sont pas cryptés. Ce service est la clinique de l’université du Québec en Outaouais.







1. Evaluation des faits et des données

Après avoir effectué l’attaque DDos transport, le temps de réponse n’arrive qu’une heure après l’attaque. Ce temps de latence entre l’attaque et la réaction est très long il pourrait porter préjudice au traitement d’admissions, pourrait créer une porte d’entrée dans le réseau car les services de contrôle de flux et d’intégrité des données seront mis hors d’état de service. Certes le service clinique n’est pas dans le même réseau que les machines de la 132.213.0.0/16 une attaque jumelée entre l’absence du cryptage des communications de celle-ci et l’attaque DDos transport car ils appartiennent tous les deux au même domaine. A côté de tout cela on a aussi constaté l’accès facile aux adresses IP malgré la présence du vpn Fortinet pptp.

1. Conclusions et prédictions des conséquences de l’activité :

Au terme de ce travail où il était question d’examiner les potentiels vulnérabilité présentent sur le site web https\\uqo.ca il en ressort principalement un constat de temps de latence très long entre une attaque DDos transport et la réaction du système de protection. Aussi l’accès aux ressources très sensibles qu’est une adresse ip ouverte à tous.

1. Recommandations d’améliorations :

* Insertion sur tous les noms de sous domaine le cryptage des messages échangés entre les navigateurs et les serveurs de domaine et sous domaine.
* Réduction de temps de réponse entre une attaque DDos et le système de sécurité de site web.
* Veille permanente de technologie de sécurité, catalogage des vulnérabilités déjà public et mise à jour régulière des logiciels.