Projet cybersecurité

Scénario

Le gouvernement du « Freedonia »[1] par la voie de son premier ministre[2] l'honorable « Rufus T. Firefly » a décidé d'offrir à son peuple un internet propre et sans danger d'interférences étrangères. Pour cette raison le gouvernement a mandaté des experts en sécurité informatique pour implanter des mécanismes de censure sur Internet.

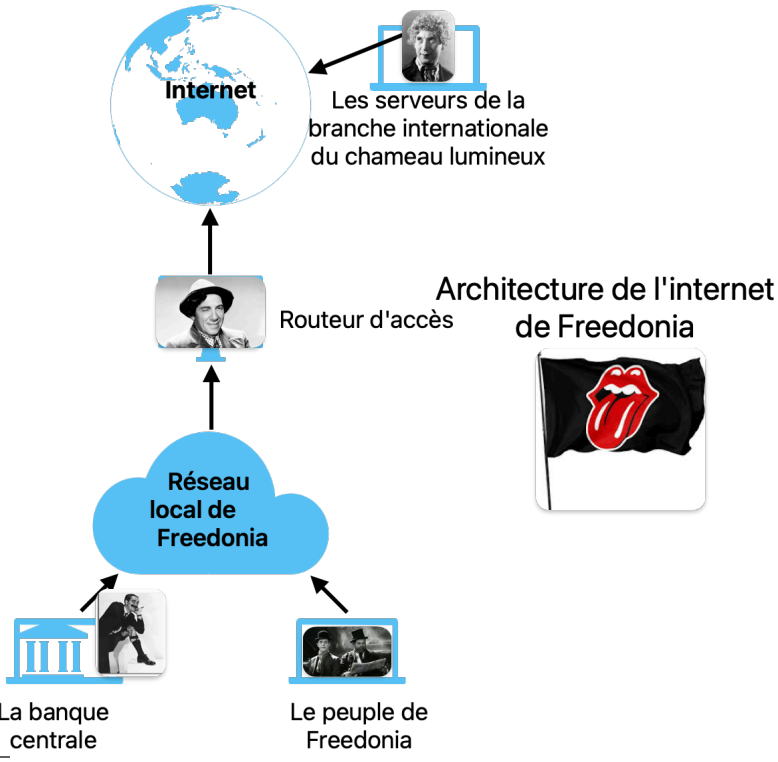
Mais le peuple de Freedonia est très attaché à la liberté d'expression, comme son hymne national peut en attester. Un groupe de révolutionnaire, va viser l'infrastructure de censure et essayer de rendre l'accès à l'internet libre. Le projet cybersécurité s'inscrit dans ce cadre.

Activités préliminaires

Nous allons constituer 6 équipes de 3 à 4 étudiants. Trois seront sous la direction de l'ingénieur en chef du gouvernement, Elchico (voir sa photo ici) et mettront en place des mécanismes de blocage d'accès, et trois seront sous la direction du chef du mouvement de libération, « le chameau lumineux », le fameux « Che Harpo »(voir sa photo ici). Les deux équipes étudieront en préliminaire les descriptions des mécanismes de censure utilisé de part le monde.

- descriptif 1 et descriptif 2

Freedonia étant un pays virtuel, son internet est aussi virtuel. Il existe donc dans l'environnement virtuel Kathara (voir ici). Nous supposerons que Freedonia à conçu son réseau afin que toutes les connexions réseau vers le monde extérieurs passent par un seul point de passage avec la topologie suivante :



[1] L'hymne national de ce charmand pays est disponible ici

[2] Vous pouvez voir son discours progressiste de politique générale ici

Les équipes de « Elchico » peuvent accéder au routeur d'accès du pays et y installer tous les outils qu'ils souhaitent. Par contre les révolutionnaires du « chameau lumineux » ne peuvent accéder au routeur d'accès, mais ils peuvent installer des machine dans le réseau local. La diaspora de Freedonia a permis à la branche internationale du « chameau lumineux » d'accéder à des serveurs dans l'internet mondial.

Actions à mettre en oeuvre par les équipes de Elchico

1- Le groupe Elchico devra configurer le routeur d'accès afin qu'il permette l'accès à l'internet réel sauf à une liste de site interdit (a trouver ici) car pouvant donner de mauvaise idées aux Freedoniens. Une série de mots-clés (voir la liste ici) sont aussi bannis et tout site contenant ces mots clés doit être filtrés.

2- Afin de pouvoir traquer le groupe dissident du « chameau lumineux », et de fournir aux forces de l'ordre les outils permettant de protéger les Freedoniens et les intérêts de la nation, le groupe Elchico mettra en place une base de données contenant toutes les connexions effectués par les freedoniens et permettant donc de surveiller qui se connecte à quel adresse sur IP et qu'est qu'il y fait.

3- le groupe Elchico doit permettre à l'ordinateur de la banque centrale et celui du premier ministre Firefly d'accéder à l'internet sans entrave car le premier ministre tient à accéder aux sites qui sont interdits à la population car il est adulte et responsable.

4- le groupe Elchico doit s'assurer de la bonne qualité de service de l'internet pour les sites autorisés et donc les délais ajouté de plus de 100 msec ne sont pas acceptables. Afin de réduire sa charge le groupe Elchico a décidé de réduire le débit de son lien vers internet à 100 Mbps. Et donc ils doivent garantir un délai < 10 msec si le traffic est inférieur à 100 mbps.

Actions à mettre en oeuvre par les équipes du chameau lumineux

1- le chameau lumineux a pour objectif de libérer le peuple de Freedonia de l'oppression de son gouvernement. Pour ceci ils trouver des moyens de court-cuiter la censure pour ceci ils vont s'appuyer sur les clients à l'intérieur du réseau local de Freedonia mais aussi sur des machines à l'extérieur du réseau local de Freedonia dans l'internet. Ils vont donc trouver des moyens de mettre en échec le filtrage par URL, par mot clé ou par adresse IP mis en place par l'équipe Elchico.

2- Le chameau lumineux veut aussi s'attaquer aux fondements de l'oppression et donc vont vouloir rendre inopérant les infrastructures de l'état Freedoniens. En particulier il vont vouloir s'attaquer à la garantie de délai < 10 msec si le débit est inférieur à 100 Mbps.

3- Le chameau lumineux veut aussi se protéger et protéger ces adhérents donc il va mettre en place des mécanismes rendant difficile pour l'équipe Elchico de les détecter dans la base de données des utilisateurs d'internet. Pour ceci le chameau lumineux s'inspire de cette citations de Mao Zedong: «Beaucoup de gens pensent qu'il est impossible pour les guérilleros d'exister longtemps derrière les lignes ennemies. Une telle croyance montre un manque de compréhension de la relation qui devrait exister entre le peuple et les troupes. Le premier peut être assimilé à l'eau, le second aux poissons qui l'habitent. Comment peut-on dire que ces deux éléments ne peuvent pas exister ensemble? »

4- Le chameau lumineux souhaiterai mettre le gouvernement Freedoniens et sont premier ministre dans l'embarras. Pour ceci il va essayer de démontrer que les équipes d'Elchico sont tous nuls et que le premier ministre firefly est un incapable. . Pour ceci elle va mettre en place un site dans l'internet ou elle affichera en temps réels le nombre de fois le chameau lumineux a permis au peuple de se connecter à un site interdit. De même l'équipe ElChico aura un site ou elle mesurera le nombre de fois ou elle a réussi à bloquer l'accès. La révolution viendra si le chameau lumineux réussi a vaincre les équipes d'Elchico.

Phases de travail

Le projet contiendra trois phases :

Phase 1- Déploiement par les équipes Elchico des mécanismes simples de filtrage DNS, par mot clé et par adresse IP. Mise en place par le chameaux lumineux de techniques simple de contournement de la censure.,

Phase 2- Adaptation du chameau lumineux aux techniques implantées par les équipes d'Elchico. Réaction des équipes de Elchico qui ont accès au compteur de succès du chameau lumineux et à leur base de données d'usage.

Phase 3-Le gouvernement devient hystérique et peu cibler les équipes du chameau lumineux. Les membres du chameau lumineux ne veulent pas être détecté et aller en prison

Librairie logicielle utile

-https://scapy.net/

-https://tateg.medium.com/capturing-network-traffic-with-python-and-tshark-19599d39dbce

-https://anvileight.com/blog/posts/simple-python-http-server/