MISSION TRAFNET

Le but de la mission Trafnet est pour nous de surveiller et comprendre pourquoi le réseau est victime de ralentissement.

Pour ce faire, nous allons analyser 2 réseaux : le vlan Labo-recherche et le réseau des BTS Sio afin de comprendre pourquoi il pourrait y avoir des ralentissements dans le réseau.

Les matériaux que nous allons utiliser sont les suivants :

* Un pc collecteur Debian qui collectera toutes les informations grâce à ntopng.
* Un switch qui nous permettra de voir tous les éléments du vlan Labo-recherche. Il nous servira aussi à voir tous ce qui se passe dans le, réseau des BTS Sio.
* Un TAP réseau qui est un dispositif permettant de surveiller un réseau informatique sans le perturber.
* Un PC qui téléchargera ou qui sera sur YouTube afin de voir qu’il prend une grosse connectivité et qu’il ralentit le réseau.

Voici la maquette de notre projet ainsi que sa réalisation :





Ntopng :

Ntopng est un logiciel permettant de surveiller le trafic sur un réseau informatique (capture et analyse de trames).

Nous avons choisi Ntopng car c’est une solution gratuite qui nous permet d’analyser et de voir tous ce qui se passe sur le réseau.

Nous l’avons installé sur la machine collecteur Debian grâce au site <https://doc.ubuntu-fr.org/ntop> qui nous a permis de connaitre les étapes de l’installation en ligne de commande ainsi que le paquet nécessaire pour l’installer.

Pour y accéder, on tape l’adresse suivante sur la barre de recherche sur n’importe quelle navigateur web : 127.0.0.1:3000

Pour se connecter l’utilisateur est : admin et le mot de passe est admin.



Voici a quoi ressemble l’interface ou l’on doit rentrer nos informations personnelles pour nous connecter.



Nous arrivons donc à l’accueil ou on voit tous le trafic qui arrive et où il va.

Maintenant nous allons vérifier l’interface sur laquelle nous souhaitons observer ce qu’il se passe :



Nous choisissons l’interface souhaiter afin de que l’on puisse voir tout le trafic qui y circule.

Pour voir un Vlan particulier nous pouvons regarder jusqu’à ce que l’on trouve une adresse particulière ou sinon il y a un moyen plus facile :



Dans la catégorie host il y a une section Vlan et dans cette section nous pouvons voir tous les Vlan présent dans le réseau et il nous suffit juste de cliquer sur le Vlan souhaité pour voir toutes les adresses présentes sur le réseau et voir ce qu’il se passe !!!

Ceci est très utile pour nous car il nous permet de trouver plus facilement le Vlan Labo-recherche et tous ce qui circule.

Pour qu’Ntopng puisse accéder au Vlan 70 nous avons décider d’utiliser un switch que nous avons configurer comme ceci.





Nous avons mis un port trunk a l’interface 1/0/1 afin que nous puissions récupérer toutes les données de la prise murale et donc du BTS Sio.

Pour accéder au Vlan Labo-recherche qui je le rappelle est le Vlan 70 Nous avons configurer l’interface 1/0/16 en mode Access sur le port 70 afin que l’on puisse seulement recevoir ce qu’il se passe sur le Vlan 70 et donc le trafic.

Afin de connaitre les commandes du switch que nous ne connaissions pas par cœur pour pouvoir le configurer nous avons utilisé le site suivant :

<https://www.clemanet.com/configuration-base-switch.php>

Ce site regroupe toutes les commandes de base que nous devons connaitre pour configurer un switch et il est utilisable et compréhensible par tout le monde.

Je n’ai pas précisé comment nous sommes aller sur l’interface du switch et bien c’est très simple.

Tout d’abord, nous avons branché un port série au switch et nous avons ensuite installé PuTTY.

PuTTY est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin, et TCP brut. Il permet également des connexions directes par liaison série.

Après avoir installé PuTTY et branché le câble série au switch, nous sommes aller sur gestionnaire de périphérique et nous avons cliqué sur port pour voir sur quel port est branché le câble série afin de savoir comment PuTTY doit faire la connexion entre le switch et notre PC.



Après vérification il s’agit du port COM8.



On n’oublie pas de cocher Sérial et on rentre Com8 dans Serial line et voila ensuite il nous suffit de valider et de mettre le mot de passe du switch qui est BTS Sio. C’est comme cela qu’on accède à l’interface du switch et que l’on fait les modifications.

Enfin nous avons utilisé un TAP réseau. Un TAP réseau est un dispositif permettant de surveiller un réseau informatique sans le perturber.

Ce périphérique matériel fournit un moyen d'accéder aux données circulant sur un réseau informatique.

Dans notre cas, le TAP va être branché entre le switch et la prise murale, ce qui va laisser passer bien sur les données mais dans le même temps les copiés vers notre collecteur ( Ntopng ) qui va ensuite les interpréter ( ce que nous faisons).

Après, il ne nous reste qu’à analyser les résultats.