Admin – troubleshooting WEB

*Situation 1 :*

***Le site web interne de l'entreprise qui vous consulte a toujours été accessible via www.formation.lab ou bien 192.168.0.4. Malheureusement, ce site n'est plus accessible aujourd'hui. Pourriez-vous jeter un coup d'œil afin de trouver une solution au problème?***

Pour commencer je démarre les serveurs DNS, le serveur dhcp. Je vérifie qu’il y a bien une connexion a internet et que la connexion intranet marche aussi. Tout est bon.

Je vérifie sur la machine web si le répertoire /etc/apache2/mods-enabled existe.

Ce n’est pas le cas donc je le crée et j’active ces modules :

a2enmod mpm\_prefork

a2enmod authz\_core

a2enmod dir

a2enmod mime

Je démarre apache2

apache2ctl start

Je fais un links <http://www.formation.lab>.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Je vais vérifier la résolution DNS en exécutant « nslookup www.formation.lab » pour voir si le nom de domaine est correctement résolu en adresse IP ainsi que « nslookup 192.168.0.4 » pour voir si l’adresse IP est associée à un nom de domaine.

Une image contenant texte, capture d’écran, Police, affichage

Description générée automatiquement  
Il semble que la résolution DNS fonctionne correctement pour le nom de domaine www.formation.lab ainsi que pour son adresse IP 192.168.0.4.

Je décide de vérifier avec Wireshark en allant faire une capture entre le client 1 et le switch. Voici ce que j'obtiens quand je fais links <http://www.formation.lab> :

A screenshot of a computer

Description automatically generated

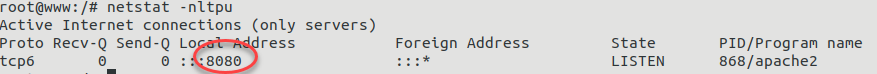
Plus précisément ceci :   
A screen shot of a computer

Description automatically generated

Ce que je constate c'est que le client a tenté de se connecter en envoyant une demande de connexion (SYN) au serveur web sur le port 80 mais il lui répond avec un signal de réinitialisation (RST) et un accusé de réception (ACK), mettant fin à la connexion.

Je peux supposer que le problème vient du fait que le port est fermé ou non écouté.

Je vais alors le vérifier avec un netstat -nltpu qui m’a permis de confirmer que le port sur lequel le serveur écoute n'est pas le bon.



J’ai donc été vérifié dans mon fichier de configuration apache2.conf.

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Le processus écoute en effet seulement sur le port 8080.

Je rajoute donc Listen 80 qui est le port par défaut.

Je tape ma commande links <http://www.formation.lab> et ça fonctionne, je tombe sur le site internet de l’entreprise.

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

*Situation 2 :*

***La page d'accueil du site web interne de l'entreprise qui vous consulte a toujours été accessible depuis www.formation.lab ou encore 192.168.0.4. Aujourd'hui, ce lien ne donne plus de résultats.... Étrange car le site reste pourtant accessible via 192.168.0.4/index.html.  Qu'a-t-il pu se passer ?***

Je démarre les serveurs DNS, le serveur dhcp. Je vérifie qu’il y a bien une connexion à internet et que la connexion intranet marche aussi. Tout est bon.

Je vérifie sur la machine web si le répertoire /etc/apache2/mods-enabled existe.

Ce n’est pas le cas donc je le crée et j’active ces modules :

a2enmod mpm\_prefork

a2enmod authz\_core

a2enmod dir

a2enmod mime

La commande links <http://www.formation.lab> ne marche pas mais celle-là oui : links <http://www.formation.lab/index.html>.

J’ai vérifié que tout marchait : le serveur répondait, la résolution des noms marchait, j’ai fait un netstat -nltpu pour m’assurer que le processus écoutait bien sur le port 80.

Je décide d'aller faire une capture Wireshark entre le client 1 et le switch.

Voici ce que j'obtiens quand je fais links <http://www.formation.lab> :

A screen shot of a computer

Description automatically generated

Comme je ne lui ai pas demandé de pages en particulier, il est censé aller me chercher la page par défaut sauf qu'ici il ne l'a apparemment pas trouvé (404 not found).

Comme ça marchait avec index.html, je me suis rappelé que dans le TP il y avait une directive qui expliquait comment faire pour avoir le fichier par défaut quand on ne spécifie pas une page précise dans l'URL, et cette directive c’est celle-ci :

* **DirectoryIndex index.html**

Je l’ai rajouté dans mon fichier de configuration comme ceci :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Ensuite j’ai simplement réessayé la commande links <http://www.formation.lab> (ou links [http://](http://www.formation.lab)192.168.0.4, et ça a fonctionné.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Voici ce que j'ai dans Wireshark quand ça fonctionne :

A screenshot of a computer screen

Description automatically generated

La seule erreur que j’ai trouvée a donc été cette directive qui indique le fichier par défaut « index.html ».