Éléments de correction : Bilan TP2 - HAProxy

Pré-requis

Le TP 1 - LAMP doit être **strictement** fonctionnel.

Objectif

Mettre en place un serveur de répartition de charge (load balancing) entre plusieurs serveurs web.

Il existe plusieurs moyen d'effectuer la répartition de charge :

- Le DNS Round-Robin (DNS RR) : Lors des résolutions de noms, le DNS fournit à chaque client une liste d'adresses IP dans un certain ordre de priorité; l'ordre changeant d'un client à l'autre.
- Le niveau TCP/IP : le client établit une connexion vers le "répartiteur" qui redirige ensuite les paquets IP entre les serveurs selon l'algorithme de répartition choisi.
- Le niveau applicatif où les requêtes sont analysées pour choisir la redirection. L'analyse porte sur les cookies (dans l'en-tête HTTP) ou l'URI (URL et ses paramètres).

Ce TP utilise HAProxy, le logiciel libre de répartition de charge le plus utilisé.

Dans ce TP, nous manipulerons plusieurs machines :

- Le serveur HAProxy qui possède 2 cartes réseaux : une sur le réseau 172.**30**.2ee.0/24 et une sur le réseau privé 172.**20**.2ee.0/24.
- Deux copies du serveur LAMP que nous basculerons tous deux sur le réseau 172.20.2ee.0/24.
- Une machine pirate que nous placerons d'abord sur un réseau, puis sur l'autre.

Pour vous aider, une annexe est mise à disposition.

⚠ TRAVAIL ATTENDU ⚠

Vous rendrez un compte-rendu respectant les conditions suivantes :

- Il doit avoir une forme professionnelle :
  - Votre document doit disposer :
    - d'un **titre**;
    - d'une **table des matières** avec numéros de pages;
    - d'une **hiérarchie de titres propre**;
    - d'une **numérotation de pages**;
    - d'un **style d'écriture homogène** (police et taille de police homogène pour un même niveau).
  - Votre document ne doit pas contenir de fautes d'orthographe.
  - Votre document ne doit pas contenir de lignes veuves ou orphelines.
- Il contient un **schéma** décrivant toutes les Machines Virtuelles utilisées, ainsi que leur adresse IP.
- Quand le sujet du TP vous demande de "mettre en place un scénario", vous devez décrire le scénario, effectuer et décrire les opérations/commandes nécessaires et joindre une capture d'écran des résultats. **Chaque scénario doit être traité en précisément une page**.
- Il est au format **pdf** et nommé ***nom*-cr-haproxy**.
- Votre nom doit figurer en première page. Le travail est individuel.
- La note de 0 pourra être attribuée en cas de non-respect d'une ou plusieurs de ces consignes.

1. Mise en place de la répartition de charge

a) Créer une nouvelle MV Debian sans interface graphique *login*-D13-haproxy avec l'adresse IP 172.30.2*ee*.2*ee* *(en provisionnement dynamique)*.
b) Ajouter une carte réseau à cette MV. Cette deuxième interface devra avoir l'adresse 172.20.2ee.2ee.
c) Créer deux copies de votre machine LAMP. Ces copies s'appelleront "*login*-D13-web1" et "*login*-D13-web2" et auront respectivement pour adresse IP 172.20.2ee.81 et 172.20.2ee.82. Ces machines n'ont pas besoin de passerelle.
d) Installer HAProxy sur le serveur HAProxy et procéder à une première configuration.

L'annexe vous donne de précieuses informations sur la configuration d'HAProxy.

e) Mettre en place un scénario montrant le fonctionnement de la répartition de charge en infligeant 2 fois plus de charge sur le premier serveur que sur le deuxième.
f) Mettre en place un scénario permettant d'obtenir des statistiques intéressantes sur la répartition de charge.

A ce stade, l'authentification sur l'appli GSB doit pouvoir causer des états incohérents.

g) Mettre en place un scénario montrant ces états incohérents.
h) Utiliser des cookies pour maintenir la connexion sur un même serveur. Mettre en place un scénario montrant que le problème est réglé.

- - - Suite à la page suivante - - -

2. Simulation d'une attaque

Slowloris est une attaque utilisant un script du même nom qui ouvre plusieurs connexions en envoyant des requêtes http partielles au compte-goutte pour conserver les connexions ouvertes le plus longtemps possible, saturant ainsi rapidement le serveur cible. C'est une attaque **DoS** (deny of service).

Slowloris essaye de garder beaucoup de connexions ouvertes avec le serveur et les conserve le plus longtemps possible. Il l'accomplit en ouvrant des connexions avec la cible et lui envoyant une requête partielle. Périodiquement il envoie des headers HTTP, mais sans terminer la requête. Les serveurs visés vont conserver leurs connexions ouvertes, remplissant leur pool de connexion concurrente, et finalement empêche des connexions ultérieures des clients.
Le principe de ce petit script Perl est d'envoyer des requêtes HTTP partielles, à intervalle régulier, afin de garder les sockets ouverts. Slowloris initie donc une requête GET vers le serveur cible, il y a un échange entre les deux entités, comme le ferait n'importe quel client HTTP vers le serveur, or ici slowloris va faire en sorte que l'échange ne se termine jamais. Slowloris ne va pas envoyer les séquences attendues par le serveur mais lui fournira de temps en temps un en-tête bidon qui sera ignoré par le serveur, mais qui permettra de maintenir la connexion TCP ouverte, empêchant ainsi le socket d'être fermé. Le serveur devient rapidement saturé, aboutissant au déni de service.
D'après Wikipédia

⚠ **ATTENTION** ⚠

Dans la suite du TP, vous allez être amené à effectuer une cyberattaque. Ce type d'attaque est interdit et vous encourez des sanctions pénales si vous procédez à ce type d'attaque en dehors du contexte du TP. Les cyberattaques ne doivent se faire que dans un **environnement de "laboratoire"** et uniquement avec l'**autorisation explicite** de votre supérieur hiérarchique ou de votre enseignant.

a) Créer une nouvelle machine virtuelle depuis le modèle **7_Modeles / SISR / DD-Modele-D6-slowloris**
*Cette machine devra être dans votre sous-dossier Services_MT et s'appellera **login-D6-slowloris**. Vous n'avez rien à personnaliser dans la configuration de cette MV sur Vcenter à l'exception du VLAN. Cette machine dispose du script slowloris et sera la machine pirate.*

b) Identifiez-vous sur la MV avec le mot de passe "mdp".

Le mot de passe administrateur sur cette MV est "PASSWORD".
Le script se lance en étant à la racine avec la commande `./slowloris.pl -dns 172.XX.2XX.XX`
Pour interrompre l'attaque, il est possible d'utiliser la combinaison Ctrl + C.

Sur un serveur web, il est possible d'utiliser la commande `ss -anp | grep 80 | wc -l` pour compter le nombre de connexions. Vous devez maîtriser le fonctionnement de cette commande.

c) Mettre en place un scénario montrant l'impact d'une *(ou plusieurs)* attaques slowloris directement sur l'un des serveurs web. *Note : Il faut choisir une adresse IP adéquate pour la MV slowloris. Pour modifier l'adresse IP de cette machine, utiliser `ifdown eth0` et `ifup eth0`.*

d) Mettre en place un scénario montrant l'impact d'une *(ou plusieurs)* attaques slowloris sur le service haproxy. *Note : Il faut choisir une adresse IP adéquate pour la MV slowloris.*

e) Éteindre et supprimer la machine slowloris du disque.

3. Bonus : inconsistance de la base de données

Les bases de données étant stockées localement sur chaque serveur, elles ne sont pas synchronisées.

a) Mettre en place un scénario montrant que les bases de données ne sont pas synchronisées.

b) Mettre en place un scénario pour apporter une solution à ce problème et montrer que la solution est fonctionnelle.