T. LA RIVIERE, M. GITTON, M. GIRARDET, F. GOT-BOUTET, N. CHALLET

TP Shellshock

Avant de commencer

1. Extraction et Installation :

L'ensemble du TP sera dans VDN. Connectez-vous sur vdn sur la machine debian-1 : (Network > Secure > debian-1), puis clonez le dépôt :

```
git clone https://github.com/tlarivier/shellshock.git
cd shellshock
```

Vous allez charger l'image Docker pré-construite :

```
docker load -i shellshock.tar.xz
```

2. Lancement du serveur :

```
docker run -d -p 5001:5001 --name shellshock shellshock:latest
```

Exercice : Opération "Ghost Protocol"

CLASSIFIED - CIA EYES ONLY

Scénario : Vous êtes un analyste de la CIA chargé d'une mission d'extraction. Nous avons un agent infiltré (nom de code "Sly Cooper") dans l'entreprise cible X.

Contexte : Notre agent a réussi à placer des informations ultra-secrètes sur un ancien serveur web de l'entreprise, mais il ne peut plus y accéder directement sans être démasqué. Votre mission est de pénétrer ce serveur depuis l'extérieur pour récupérer ces données cruciales.

Informations : Le serveur utilise une version obsolète de Bash vulnérable au CVE-2014-6271 (Shellshock). Notre agent a caché les informations dans le répertoire personnel de l'utilisateur `www-data`.

Mission : Exploiter la vulnérabilité Shellshock pour accéder au système et récupérer :

— Le **message secret** de notre agent infiltré

Attention : Cette mission est hautement classifiée. Aucune trace ne doit être laissée.

Infiltration

1. Désactiver les proxy http_proxy et https_proxy.
2. Consulter le serveur en allant sur la page http ://localhost :5001.
3. C'est à cette étape que votre travail commence.

À l'aide de la commande suivante :

```
curl -H "<HEADER>: () { :; }; <COMMAND>;" <URL>
```

récupérez les informations suivantes :

— L'utilisateur courant du serveur

— La version de bash

Maintenant que vous avez établi un accès au système, votre objectif principal est de localiser et récupérer le message de notre agent infiltré "Sly Cooper".

4. Localiser et récupérer le message de notre agent infiltré "Sly Cooper".

Couverture : Bonus

Détection

Maintenant que vous avez récupéré les informations, vous devez vous assurer que votre opération est couverte. Connectez-vous au conteneur Docker et analysez les logs Apache pour détecter les traces de l'attaque. Quelles commandes utiliser pour identifier les requêtes malveillantes dans les logs ?

Défense

Proposez deux méthodes de protection :

1. Filtrage Apache : Quelle directive Apache permet de supprimer les en-têtes contenant le pattern Shellshock ?

2. Mise à jour système : Comment remplacer la version vulnérable de Bash ? Comment tester que la vulnérabilité n'est plus présente ?

Testez vos contre-mesures et vérifiez qu'elles bloquent la faille précédente.

Bravo agent, vous avez terminé votre mission avec succès !