CS Games 2017

Rétro-ingénierie

Participants	2
Stations	1
Valeur	6%
Durée	3 heures

Rétro-ingénierie

Mise en Situation

En 2013, le génie de l'informatique Edouard Kropotkin quitta sa Russie natale pour démarrer son entreprise de rêve à Silicon Valley. Il engagea comptables, réceptionnistes et baristas, mais demeura le seul développeur de la boîte.

Les semaines se succédèrent, où tous les employés travaillèrent leurs mouvements de ping-pong et leurs habiletés de Mario Kart, jusqu'au jour où ce fût trop. Épuisé d'être le seul à produire des résultats, Edouard s'exila dans une commune anarchiste autogérée, laissant tous ses rêves de startups à ses anciens collègues.

Le problème, c'est que sans lui, personne ne peut faire fonctionner l'entreprise! Édouard utilisait des logiciels qu'il avait créé lui-même et il s'est envolé avec les sources.

Tâches

Tâche 1 - Transfert de fichiers

Introduction

Catégorie Implémentation/Protocole

Avant sa disparition, Edouard travaillait sur un système de transfert de fichiers. Tout porte à croire qu'il a seulement eu le temps de coder la portion serveur. Si nous voulons vendre ce produit, vous devez nous construire un client!

Le langage utilisé importe peu!

Description Technique

Vous possédez une copie locale d'un binaire capable de servir des fichiers par le réseau. Vous devez coder un client capable d'interagir avec lui.

- Vous devez trouver comment vous authentifier au serveur
- Vous devez obtenir la liste des fichiers à télécharger
- Vous devez télécharger un fichier hébergé sur le serveur
- Vous devez téléverser un fichier de votre disque vers le serveur
- Toutes les tâches doivent se terminer de façon propre (pas de paquet inattendu ou de connexion qui prend fin sans avertissement)

Ce que vous possédez:

Vous possédez les fichiers et dossiers suivants:

- server_folder/ contient les fichiers et dossiers hébergés sur le serveur
    - srv/
        - Représente la racine du serveur de fichiers. Il doit être dans le même dossier que “server”. Il contient les fichiers pouvant être servis aux clients. C'est aussi là qu'atterrissent les fichiers téléversés.
    - server
        - Il s'agit du binaire serveur à effectuer la rétro-ingénierie. Comprenez son fonctionnement pour créer un client.
        - Il gère les fichiers dans srv/. Lors de la correction, il sera sur un serveur distant.
- client_folder/ contient les fichiers et dossiers du client
    - local/
        - Contient vos fichiers locaux. C'est là que vous devez sauvegarder vos fichiers téléchargés.
    - client
        - Il est **vide**. C'est à **vous** de le remplacer par un script ou un exécutable. Ce qu'il reçoit du serveur doit être écrit dans stdout.
    - run.sh
        - Votre outil pour vous corriger. Vous pouvez le lancer avec ./run.sh <username> <password>. Il va effectuer 3 commandes. **Ces trois commandes sont celles que vous devez implémenter dans client**:
            - Tenter de lister les fichiers sur le serveur
            - Tenter de télécharger un fichier du serveur (srv/) vers un dossier local (local/)
            - Tenter de téléverser un fichier local (dossier local) vers le serveur (srv)

Les commandes à implémenter

- Lister les fichiers distants
    - $./client <ip> <nom d'utilisateur> <mot de passe> list_files
- Télécharger un fichier distant
    - $./client <ip> <nom d'utilisateur> <mot de passe> download <nom du fichier>
- Téléverser un fichier local
    - $./client <ip> <nom d'utilisateur> <mot de passe> upload <nom du fichier>

Pratique

Phase	Tâche	Pts
Lister les fichiers distants	Vous êtes authentifié par le serveur	/2
	Vous obtenez la liste des fichiers du serveur (le contenu de srv/)	/2
	Vous quittez la communication de façon propre	/1
Vous téléchargez un fichier distant	Le fichier téléchargé dans local/ est identique à l'original dans srv/	/3
	Vous quittez la communication de façon propre	/1
Vous téléversez un fichier local	Le fichier téléversé dans srv/ est identique à l'original dans local/	/3
	Vous quittez la communication de façon propre	/1

- Toute communication entre client et serveur doit être faite par le lien réseau.
- Il est interdit de modifier le serveur. Vous devez seulement créer un client.

Théorique

A) **Donnez la combinaison <utilisateur>:<mot de passe> acceptée pour l'authentification.**

Nom d'utilisateur	Mot de passe	Pts
		/2

B) **Quel est le protocole de communication réseau utilisé par le serveur fourni?**

Réponse: _____ /1

C) **Sur quel port écoute-t-il?**

Réponse: _____ /1

Bonus

A) **Une vulnérabilité est présente dans la fonction de téléchargement. Quelle est-elle?**
Réponse: _____ /1

B) **Comment la corriger?**
Réponse: _____ /1

C) **Remettez une preuve de concept afin de vous emparer du fichier /etc/passwd.**
/1

Tâche 2 - Liste de clients

Introduction

Catégorie Crypto/Scripting

Edouard avait monté une liste de possibles clients intéressés par nos produits. La valeur de cette liste est inestimable, c'est pourquoi il la gardait encryptée. Le hic, c'est qu'il ne semble pas y avoir de programme de déchiffrement, seulement un script de chiffrement difficile à lire. On pense que la clé était dérivée d'une photo, mais cette dernière reste introuvable.

Description Technique

Vous possédez une liste encryptée ainsi qu'un script de chiffrement. À vous de coder un script afin de déchiffrer la liste!

Ce que vous possédez:

- encrypt_list.py
    - Le script d'encryption utilisé
- o.enc
    - La liste à déchiffrer

Pratique

Tâche	Pts
Fournir un script de déchiffrement	/10

Tâche 3 - Gestionnaire de mots de passe

Introduction

Catégorie Patching

Nous utilisons beaucoup Instagram, mais impossible de se souvenir de notre mot de passe! Edouard nous a donc créé un gestionnaire. Lorsqu'on lui fourni le master-password, le logiciel nous affiche le mot de passe que nous utilisons sur Instagram. Pour être certain que personne n'y accède sans autorisation, le gestionnaire est rempli de mesures de sécurité.

Il ne peut être roulé que sur l'ordinateur d'Edouard et prend plusieurs heures à s'exécuter!

Nous avons besoin de faire une publication Instagram le plus rapidement possible! Ça urge!

Description technique

Le mot de passe Instagram de l'entreprise est gardé dans un gestionnaire de mots de passe. S'inspirant de l'ouverture à délai des coffres de banque, on n'obtient le mot de passe que plusieurs heures après avoir exécuté le gestionnaire. D'autres mécanismes ont aussi été mis en place pour s'assurer que personne ne puisse avoir accès à ces informations

Ce que vous possédez:

- pwManager
    - Le gestionnaire. Il peut être lancé dans la fenêtre de commande avec $./pwManager <mot de passe>

Pratique

Tâche	Pts
Remettez une version patchée du gestionnaire qui affiche instantanément le mot de passe (Moins vous changez d'octets, plus vous faites de points)	/6

Formule utilisée: *nombre_octets / minimum * 6*

Théorique

A) Quel est le mot de passe du compte Instagram?

Réponse: _____ /4