Exploit

Mise au sol d'un binaire

- labexploit -
pedagogie@ecole-89.com

Table des matières

Détails administratifs

Votre travail doit être **envoyé sur la forge logicielle**. Le nom de votre dépôt doit être `2021_exploit`. Un nom de dépôt erroné donnera lieu à un échec du projet.

Vous devez donner le droit en lecture à l'utilisateur `delivery-collector`, qui sera chargé de ramasser votre travail pour le corriger.

Vos identifiants de connexion à la forge sont votre mot de passe LDAP/UNIX, tel qu'il fonctionne sur les postes de l'école.

Médailles accessibles :

Rendu Git :
Vous avez réussi à rendre votre travail sur la forge logicielle

Prémisse

Ce projet à plusieurs objectifs : vous faire découvrir des failles de sécurité dans un binaire en C, vous faire écrire de la documentation sur ses failles et vous les faire corriger.

En sécurité on distingue les intrusions de systèmes dits « boite noire » et « boite blanche ». Les boites noires sont des systèmes dont les attaquant n'ont pas de connaissance préalable. Au contraire les tests sur boites blanches requièrent la connaissance du code cible.

Ce projet se réalise à la façon d'une boite blanche, car une copie du code exécutée vous est fournie ici. Le code en production est sûr `172.17.250.100:1234` au château. L'hôte est accessible depuis une session SSH étudiant.

Exploitations

Le but du projet est de trouver des drapeaux – *flags* – au format : `FLAG{123456ABCDEF}` sur une instance du programme que l'on maintiendra en ligne. Pour ce faire, vous devez trouver des failles dans le programme et les exploiter sur l'instance en production.

Le mieux reste de faire la recherche de failles en local sur votre ordinateur.

L'utilisation d'outils de tests de pénétration est inerdite. Tout comme le *brute force*.

En cas d'erreur, le service en production est supposé redémarrer, mais pour éviter de pénaliser les autres participant·e·s, évitez de provoquer trop de mises en panne.

Médailles

Chaque type d'exploitation réussie et documentée donne lieu à une médaille. Liste de médailles accessible, non-exhaustive :

– abus de chemin relatifs ;
– abus de descripteurs de fichiers ;
– dépassement de tampon ;
– injection de commande ;
– injection de programme.

Corrections

En plus de repérer des failles, vous devez proposer des corrections pour sécuriser le programme face à elles.

Pour ce faire, corrigez directement les failles dans le code, faites de nouveaux commits et poussez-les sur un dépôt spécial `2021_exploit_server`, sur lequel le robot de rendu doit avoir les privilèges en lecture.

Documentez les corrections que vous avez faites dans un `readme.md`. Chaque correction donnera lieu à une médaille, en fonction du type de faille dont il est question.

Rendu

L'organisation du rendu est libre, vous devez faire au moins un fichier markdown, contenant les drapeaux que vous avez trouvés, ainsi que les explications nécessaires à reproduire les failles que vous avez exploitées.

Si vous avez produit des scripts, ou des programmes pour exploiter des failles, vous devez également les rendre ici. Aucun binaire pré-compilé ne doit être rendu, seulement le code source.

Nature du binaire

Le programme que l'on vous fournit est un serveur TCP sur lequel il est possible lister, créer et afficher des messages. Les messages avec le préfixe `[admin]` nécessitent un accès privilégié, mais peuvent être écrits par tous. Les messages son simplement une suite de caractères.

Le protocole de communication est défini dans le fichier `proto.md`.