TP débordement

Sécurité des entrées utilisateurs

- DaemonLab -
pedagogie@ecole-89.com

Tu pousses le bouchon un peu trop loin Maurice.

Table des matières

Détails administratifs....3
Prémisse....4
Exercice....4

Détails administratifs

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

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

Médailles du TP

- « buffer overflow simple exploit »
- « write anything »
- « good readme »

Prémisse

Le *buffer overflow* est un phénomène fréquent en programmation, dès lors que l'on est incertains sur la façon dont on doit gérer la mémoire, ou en cas d'inattention. Les dépassements de mémoire sont des fautes qui peuvent être exploitées par un utilisateur malveillant pour potentiellement faire tomber votre programme, ou pour accéder à des données supposées être cachées.

Une attaque de *buffer overflow* va profiter d'un tampon qui n'est pas sécurisé pour tromper le programme en modifiant d'autres valeurs, plus loin en mémoire ; permettant ainsi l'injection de code ou simplement la modification de son comportement.

Exercice

Votre but est de compiler ce programme, de l'exécuter et de « devenir admin » sans connaître le mot de passe, qui — de toute façon – est généré aléatoirement.

Pour avoir réussi, il faut que le programme finisse par afficher le message de bienvenue pour l'administrateur.

L'exploitation du programme peut être faite à l'aide d'un programme de votre conception et exclusivement à l'aide d'une fonction `main` et de quelques appels à `write`.

> Notez qu'en C il est possible d'écrire ou de lire tout et n'importe quoi du moment que le compte d'octets est bon. Les appels systèmes ne se limitent pas aux chaînes de caractères et cela peut être très pratique.

Rendu

Le rendu se fait sous forme libre. Rendez le code dont vous vous êtes servis pour exploiter le programme, ainsi qu'un `readme` avec les explications de ce que vous avez fait et les instructions pour reproduire votre manipulation.