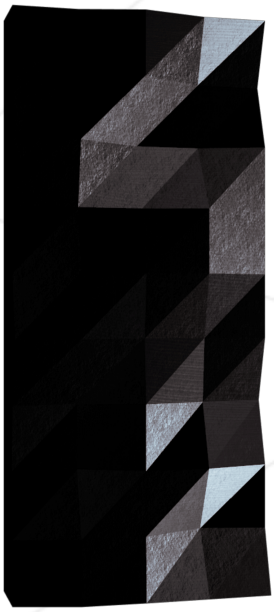

Root-Me / App - Système

Vulnérabilité sur les binaires ELF

42 staff staff@42.fr

Résumé: Ce projet a pour but de vous familiariser avec **ELF32** *en vous faisant participer au challenge Root-Me.*

Table des matières

Chapitre I

Préambule

ELF (Executable and Linkable Format, format exécutable et liable ; anciennement Executable and Linking Format) est un format de fichier binaire utilisé pour l'enregistrement de code compilé (objets, exécutables, bibliothèques de fonctions). Il a été développé par l'USL (Unix System Laboratories) pour remplacer les anciens formats a.out et COFF qui avaient atteint leurs limites. Aujourd'hui, ce format est utilisé dans la plupart des systèmes d'exploitation de type Unix (GNU/Linux, Solaris, IRIX, System V, BSD), à l'exception de Mac OS X.

Wikipedia

Chapitre II

Root-Me

II.1 Introduction

Root-Me est un challenge en ligne qui vous propose des épreuves sur le thème de la sécurité avec une difficulté graduelle et un environnement adapté, idéal à l'apprentissage. Nous vous proposons donc de participer à ce challenge en l'intégrant aux projets de l'école. L'intégralité des contenus Root-Me sont la propriété de leurs auteurs conformément aux mentions légales de root-me.org.

II.2 Root-Me / App - Système

Root-Me propose un grand nombre d'épreuves différentes rassemblées par thèmes. Le thème que nous avons choisi pour ce projet 42 est App - Système.

Ce challenge propose des épreuves de difficulté croissante que vous devez résoudre pour valider ce projet.

II.3 Inscription sur Root-Me

Pour participer à ce projet, en plus de l'inscription ordinaire sur l'intranet, vous devez créer un compte sur Root-Me. Avant de procéder, veuillez-lire attentivement les consignes suivantes :

- Veuillez **impérativement** lire les mentions légales de Root-Me. Oui, en entier. Participer à ce projet sous-entend l'acceptation sans conditions de ces mentions légales. Dans le cas contraire, 42 ne reconnaît pas votre participation à Root-Me.
- Pour limiter la fraude et l'usurpation d'identité, ainsi que pour valider votre travail à 42, nous vous imposons le nom d'utilisateur de votre compte Root-Me pour ce projet. Votre nom d'utilisateur doit impérativement être **votre login suivi de 42**. Par exemple : qperez42, dgiron42, ... Dans le cas improbable où votre nom d'utilisateur serait refusé par Root-Me, veuillez prendre contact avec l'équipe pédagogique au plus vite.
- Si vous possédez déja un compte personnel sur Root-Me, vous devez quand même en créer un nouveau respectant la consigne précédente. Cela signifie que vous ne

pouvez pas utiliser votre compte personnel pour participer à ce projet. Toutefois, vous pouvez bien entendu importer vos solutions existantes depuis votre compte personnel vers votre compte 42 et reprendre là où vous en étiez.

Chapitre III

Le projet

III.1 Objectifs

Ce projet a pour but de vous faire découvrir comment détecter et exploiter des vulnérabilités applicatives sur `ELF`. Le challenge `Root-Me` / App - Système vous propose une série dépreuves de difficulté croissante que vous devez réussir pour valider ce projet.

Pour cela, vous devrez vous dépasser et faire preuve de persévérance. `Root-Me` met à la disposition de ses utilisateurs de la documentation qui fera un excellent point de départ. Bien entendu, une connaissance minimum en `C`, en assembleur et de `gdb` est obligatoire. Mais cela ne devrait pas vous poser de problème, non ?

III.2 Partie obligatoire

Les challenges ci-dessous constituent la partie obligatoire de ce projet. La plupart de ces challenges se situent dans la partie `Root-Me` / App - Système, quand ce n'est pas le cas leur catégorie est indiquée entre parenthèses.

Voici la liste des challenges obligatoires :

- ELF32 - System 1 (`Root-Me` / App - Script)
- ELF32 - System 2 (`Root-Me` / App - Script)
- ELF32 - Chiffrement avec le PID (`Root-Me` / Cryptanalyse)
- ELF32 - Format string bug basic 1
- ELF32 - Stack buffer overflow basic 1
- ELF64 - Stack buffer overflow basic
- ELF32 - Stack buffer overflow basic 2
- ELF32 - BSS buffer overflow
- ELF32 - Stack buffer overflow basic 4
- ELF32 - Race condition
- ELF32 - Stack buffer and integer overflow
- ELF32 - Stack buffer overflow 5
- ELF32 - Remote BSS buffer overflow
- ELF32 - Remote Format String bug

III.3 Partie bonus

Vous connaissant, vous n'allez faire qu'une bouchée de ces premiers challenges, n'est-ce pas ? En conséquence, les 7 derniers constituent la partie bonus de ce projet. C'est-à-dire :

- Hardened binary 1
- Hardened binary 2
- Hardened binary 3
- Hardened binary 4
- Hardened binary 5
- Hardened binary 6
- Hardened binary 7

III.4 Rendu et évaluation

La nature externe de ce projet implique un rendu de votre travail légèrement différent de vos habitudes.

- Vos solutions sont bien entendu à soumettre sur `Root-Me` pour validation des challenges. Toutefois, vous devez également pusher une copie de vos solutions sur votre dépôt de rendu sur la `vogsphere`. Sous entendu les commandes qui vous ont permis de résoudre le challenge.
- Lors de la peer-évaluation, un challenge validé sur `Root-Me`, mais dont la solution est absente de votre dépôt ne sera pas comptabilisé. Soyez méticuleux.
- Nous n'imposons pas de convention de nommage particulière, toutefois prenez soin de créer un dossier différent par challenge à la racine de votre dépôt avec un nom qui permet d'identifier clairement et simplement de quel challenge il s'agit. Votre solution sera alors placée dans ce dossier.

III.5 Image de l'école

Je sais que cela est superflu car vous êtes tous gentils et bien élevés, mais il va de soit que vous devez vous montrer polis et courtois en toute occasion avec la communauté `Root-Me`. Les règles de `Root-Me` s'appliquent `de-facto` en plus des règles de ce projet. N'oubliez pas que vous engagez votre responsabilité auprès de `Root-Me` en plus de votre engagement auprès de l'école. Si à cause d'un comportement discutable `Root-Me` interdit l'accès à nos étudiants, vous serez les perdants.

Mais trève de mauvaises pensées, vous allez être brillants, j'en suis sincèrement convaincu. Je compte sur vous pour gagner l'estime de la communauté `Root-Me` et faire rayonner l'école.

Pour terminer, si quelqu'un du staff `Root-Me` lit ce document et souhaite prendre contact avec notre équipe au sujet de nos étudiants, vous pouvez me contacter directement à l'adresse thor@staff.42.fr.