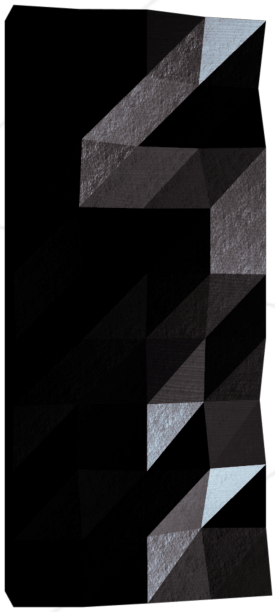

Bootcamp Cybersecurité | 42

tsunami

Résumé: Dépassements de tampon

Version: 1

Table des matières

Chapitre I

Introduction

Depuis qu'Aleph1 a créé son "Smashing The Stack For Fun And Profit" il y a plusieurs dizaines d'années, les débordements de tampon et de pile sont une technique bien connue qui est toujours à l'origine de la plupart des vulnérabilités les plus utilisées par les attaquants. Créez un programme C qui provoque un simple dépassement de tampon dans un environnement Windows XP 32 bits. Pour ce faire, vous utiliserez la fonction strcpy.

Chapitre II

Instructions générales

Pour ce projet, vous utiliserez le langage de programmation C pour le programme vulnérable. Afin d'exécuter ce type d'exploit, vous aurez besoin d'un environnement vulnérable : Windows XP. Vous pouvez utiliser une machine virtuelle Vagrant, par exemple, celle-ci.

Une fois que vous avez créé l'exécutable vulnérable, vous allez construire une charge utile qui profitera du programme pour exécuter du code.

Chapitre III

Partie obligatoire

La procédure est basée sur deux phases, la création du programme vulnérable et la construction de la charge utile qui lui sera envoyée lors de l'exécution. Après avoir créé et vérifié que l'application développée est vulnérable, il est temps de créer un exploit qui permet de tirer parti de cette vulnérabilité. Pour cela, il faut suivre les étapes suivantes :

- Création de l'exploit. Le programme sera appelé `tsunami.exe` et recevra un seul paramètre comme argument.
- Création d'une charge utile, qui ouvrira automatiquement la calculatrice de Windows XP lorsque la vulnérabilité sera exploitée.
- La charge utile doit contenir le code à exécuter dans le shellcode. Construire votre propre charge utile est une partie fondamentale de la technique. Documentez-vous pour analyser et comprendre ce que sont les existants, mais essayez de développer votre propre charge utile au lieu de vous rendre à Shell-storm.

Chapitre IV

Partie bonus

L'évaluation des bonus se fera `SI ET SEULEMENT SI` la partie obligatoire est `PARFAITE`. Dans le cas contraire, les bonus seront totalement `IGNORÉES`.

Vous pouvez améliorer votre projet grâce aux fonctionnalités suivantes :

- Développement du même système (programme et charge utile vulnérables) dans un environnement Linux vulnérable.
- Développement du même système sous Windows, mais en utilisant un langage de programmation différent du C.

Chapitre V

Évaluations peer 2 peer

Ce projet sera corrigé par d'autres étudiants. Remettez les fichiers dans le dépôt Git et assurez-vous que tout fonctionne comme prévu.