TP ROW HAMMER

Sécurité

Membres :
Bonneau Baptiste
Centeno Matéo
Ferreira Pierre
Jean Mathilde
Zborowski Lucas

Contexte
Vous faites partie d'une équipe de hackers d'élite engagée par une organisation secrète. Votre mission, si vous l'acceptez, consiste à exploiter la faille de sécurité Row Hammer sur un serveur appartenant à une entreprise rivale, connue sous le nom de “asaN”. La asaN détient des informations confidentielles qui pourraient compromettre la sécurité nationale, et votre organisation a été chargée de les récupérer.

Vous avez 30 minutes pour infiltrer le serveur de la asaN en utilisant l'attaque Rowhammer, tout en évitant de vous faire détecter. Soyez conscients que vous agissez dans une zone juridiquement grise et que les conséquences de votre mission peuvent être graves si vous êtes pris.

Rappel
Pour rappel, l'attaque Row Hammer est une vulnérabilité matérielle qui se produit lorsque des opérations de lecture et d'écriture fréquentes et rapides sont exécutées sur des lignes adjacentes de cellules de mémoire (ou "rows") dans une puce de RAM. Cette activité intensive peut provoquer des interférences électromagnétiques qui altèrent les données stockées dans les cellules de mémoire adjacentes, permettant ainsi à un attaquant de corrompre ou de manipuler des données en exploitant cette faiblesse.

Partie 1: Mise en bouche

1) Memory Game

Vous avez à disposition un programme d’initialisation aux hackers, `HowRHWork.py`, les règles sont plutôt simples, vous devez trouver à quelle ligne il y a eu un bit flipé. Pour cela, vous avez 4 options :

- 1 : Afficher l'état actuel de la mémoire
- 2 : Marteler : À l'aide d’un puissant coup de marteau, tentez de faire changer la valeur d’un bit en mémoire. Attention, ce processus ne marchera pas à tous les coups.
- 3 : Submit : soumettez votre réponse, il s’agit du seul moyen de vaincre l’exercice, vous devez entrer la ligne à laquelle le bit a changé de valeur.
- 4 : Retour : Abandon total de l’attaque.

Ce cours programme n'est qu'une simulation de RowHammer et n'est en rien dangereux pour le pc, il s'agit d'un exercice cours, pour comprendre les bases de l'attaque de Rowhammer.

P.S : Il vous sera probablement nécessaire d'installer la librairie "*colorama*" de python pour faciliter la complétion de cet exercice.

2) Le code Corrompu

Sur le dépôt Code#0, une source fiable vous a fourni un code non complet, ce code est capable de simuler une attaque RowHammer. Malheureusement, ce code a été corrompu, et seuls certains des commentaires de documentations pourront vous permettre de remplir ces trous. Vous retrouverez ce document dans `~/Top_Secret/CorruptedCode`. Il ne sera pas forcément utile de tester votre code jusqu'à l'apparition d'un message "`Oui, un bit a flippé en mémoire.`" car ce processus peut être beaucoup trop long, vous n'aurez uniquement besoin de compléter les trous du codes représentés par `/***/`.
Bonne chance, vous en aurez besoin.

Partie 2 : Test de Rowhammer par Google

Vous venez de découvrir que votre fidèle allié Google a mis à disposition un code permettant de créer une attaque Row Hammer. Étant donné que votre code n'est pas super performant, lancez une attaque en utilisant ce nouveau programme.

A réaliser sur VDN

1) Par magie, vous avez eu accès à un ordinateur et vous devez récupérer des informations sur l'ordinateur. Recherchez des informations sur la RAM utilisée sur cet ordinateur. *Votre intuition révèle l'existence de la commande dmidecode.*

2) Votre allié vous a fourni le code source présent au repository suivant :
https://github.com/google/rowhammer-test.git

3) Démarrez l'attaque avec **./make.sh** puis **./rowhammer_test**
Qu'observez-vous ?
Il vous faudra sûrement plusieurs heures avant de trouver une faille avec ce programme ! Il est temps d'essayer autre chose ! Éteignez-le.

4) Votre programme s'est arrêté !

   Que s'est-il passé ?
   Qu'elle est l'adresse obtenue et qu'elle est celle que nous devions avoir par défaut ?