Rapport de Solution : MasterKee

Catégorie : Forensic (Analyse Mémoire) **Vulnérabilité exploitée :** CVE-2023-32784 (KeePass 2.x)

1. Analyse du problème

Le challenge fournit un dump mémoire (.DMP) d'une machine Windows. L'objectif est d'extraire le **Master Password** d'une base de données KeePass.

L'analyse de la sécurité récente de KeePass révèle une faille (CVE-2023-32784) dans le composant SecureTextBoxEx. Lorsqu'un utilisateur tape son mot de passe, chaque caractère est temporairement stocké en mémoire aux côtés d'un caractère de "masquage" (le fameux point ●), laissant des résidus même après la fermeture de la base.

2. Méthodologie Technique

La technique repose sur la recherche de patterns binaires spécifiques (artefacts) laissés dans la RAM.

Le Pattern "Magique" : Dans la mémoire gérée par .NET pour KeePass, le caractère de masquage ● est encodé par les octets 0xCF 0x25. Le bug fait que chaque lettre tapée se retrouve souvent adjacente à ce pattern.

Fonctionnement du script (solve.py) :

1. **Lecture Binaire :** Le script ouvre le fichier .DMP en mode binaire.
2. **Scanning :** Il parcourt la mémoire octet par octet à la recherche de la séquence 0xCF 0x25 suivie d'un caractère ASCII imprimable.
3. **Agrégation :** Il collecte toutes les occurrences trouvées.
4. **Reconstruction :** En analysant la position des caractères trouvés, il reconstitue les lettres probables du mot de passe.