Simulation d'une attaque Meltdown

Nathan Verdier, Chloé Mourgand, Thomas Chazot, Lucie Bedouret, Rémi Regnault

Mise en situation

Petit hacker que vous êtes devenu au fil des TP de sécurité, vous avez découvert qu'un dépôt github privé contient des images d'une star que Jonathan adore. Seulement il ne veut pas vous dire de qui il s'agit, donc vous voulez le découvrir par vous même, par tout les moyens.

Vous savez que l'adresse du dépôt en question est `https://github.com/jonathanGrosBg/MySecretRepository.git`, et vous savez que Jonathan, la personne ayant créé le dépôt, a rentré les mots de passe de son adresse mail et de son compte github dans un fichier sur sa machine.

L'idée vous vient alors de monter une attaque Meltdown sur la machine de Jonathan pour vous permettre de récupérer la mémoire de sa machine.

Vous pourrez alors récupérer les comptes de Jonathan en scannant les adresses mémoires, vous permettant de cloner le dépôt à votre tour.

Comment procéder ?

Il faut monter l'attaque Meltdown. Pour ce faire, nous vous mettons à disposition le code python suivant, qui vous permet de simuler une attaque Meltdown sur la machine de Jonathan.

Cependant, ce code ne permet que de récupérer les données à une **(et une seule)** adresse mémoire en hexadécimal (qui commence à 1). Il va donc falloir que vous utilisiez ce code à bon escient pour vous permettre de récupérer la totalité de la mémoire et la mettre dans un fichier texte. Si l'adresse mémoire que vous visez n'existe pas le programme vous retournera une exception.

> **Attention !** Si la partie de l'exécution spéculative se termine avant que vous n'ayez pu récupérer les données à l'adresse voulue, vous ne récupèrerez rien, et vous manquerez peut-être l'accès au dépôt !!! (le programme retournera alors une exeption)

Pour utiliser le programme python, vous pouvez utiliser la ligne de commande: `python3 Meltdown.py adresse` Afin de l'utilisez dans votre programme python, nous vous conseillons de jeter un oeil à la librairie subprocess.

Une fois chose faite, vous n'aurez plus qu'à convertir le fichier binaire obtenu en ASCII, et parcourir la mémoire jusqu'à trouver l'espace mémoire contenant les identifiants de Jonathan.

Une fois ceci fait, vous n'aurez plus qu'à vous connecter à l'adresse mail de Jonathan et de vous connecter à son compte github pour récupérer et cloner le dépôt.

Et voilà ! Vous pouvez maintenant admirer les photos de votre star préférée