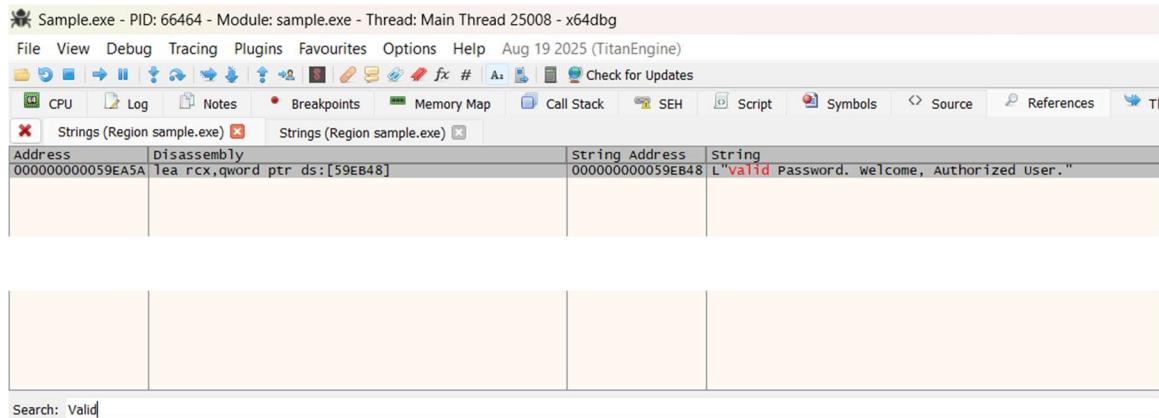


6GEI186 - Architecture des ordinateurs**BONUS : Travail 4 – Trouver le Mot de passe Original du Programme****Remis à : Prof. Jérémy Bouchard****Par:****David Chalons – CHAD17070000****Mobina Shamsadini – SHAM1352060****Samara Boudreault – BOUS08610400**

Bonus : Trouver le Mot de passe Original du Programme

Explication de la démarche utilisée

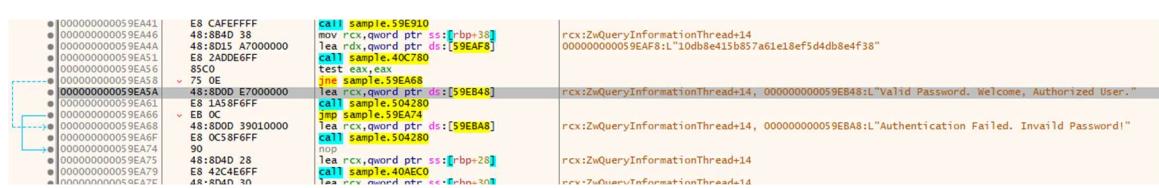
Premièrement, nous avons localisé l'endroit où se trouve le message de succès « Valid Password. Welcome, Authorized User. » à l'aide de l'option **Az** (recherche de chaînes de caractères) dans x64dbg.



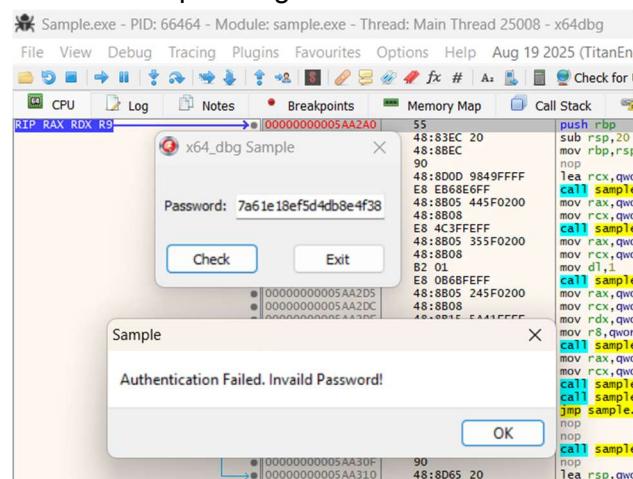
Address	Disassembly	String Address	String
000000000059EA5A	lea rdx,qword ptr ds:[59EB48]	000000000059EA5A	L"Valid Password. welcome, Authorized User."

Search: Valid

Region Search 100%



Par la suite, nous avons analysé les instructions qui gèrent la saisie du mot de passe et nous avons également remarqué une instruction *lea* qui charge dans *rdx* l'adresse d'une chaîne de caractères constants. Cette chaîne est ensuite utilisée dans un appel de fonction où elle est comparée avec la valeur de l'entrée utilisateur. Nous en avons conclu que la valeur pointée par *rdx* représentait la référence utilisée pour valider le mot de passe.



En observant cette chaîne, nous avons constaté qu'il s'agissait d'une suite de 32 caractères hexadécimaux. En la testant directement comme mot de passe, cela ne fonctionnait pas, ce qui confirmait qu'il ne s'agissait pas du mot de passe en clair, mais d'un hash.

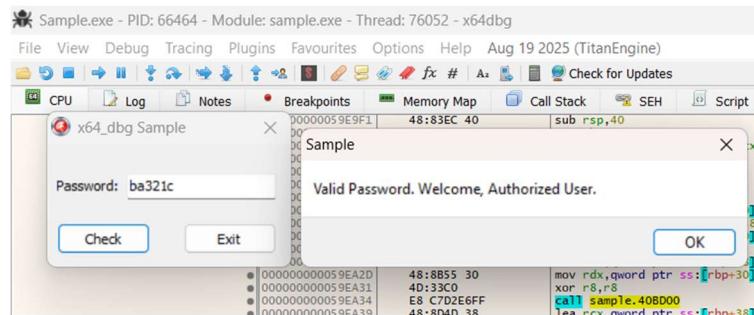
Avec un site¹ pour détecter quel type d'encryptions c'était nous avons trouvé hash MD5.

Nous avons ensuite copié cette valeur de hachage et l'avons soumise au site *HashLookUp*², qui nous a retourné la chaîne de caractères suivants : « ba321c ». Enfin, après avoir essayé « ba321c » dans le programme original (non modifié), nous avons confirmé qu'il s'agissait bien du mot de passe correct.

The screenshot shows the HashLookUp interface. At the top, it says "Possible identifications: Decrypt Hashes". Below that, the hash value "10db8e415b857a61e18ef5d4db8e4f38" is entered, with a note that possible algorithms include MD5, SHA1.Substr(0, 32), MD4, NTLM, md5(md5(\$plaintext)), md5(md5(\$plaintext)...\$plaintext), and md5(md5(md5(\$plaintext))). A large blue button with a magnifying glass icon and the hash value is prominently displayed in the center.

Result

Hash	Password	Sources	Loaded password lists
10db8e415b857a61e18ef5d4db8e4f38	ba321c	RockYou2021	SecList Top 100 SecList Top 500 SecList Top 1000 SecList Top 10000



¹ https://hashes.com/en/tools/hash_identifier

² <https://binsec.tools/lookup/hash/>