Info:

The Redteam found a seemingly very valuable binary. It looks like to be some sort of Password-Safe but we are missing the password

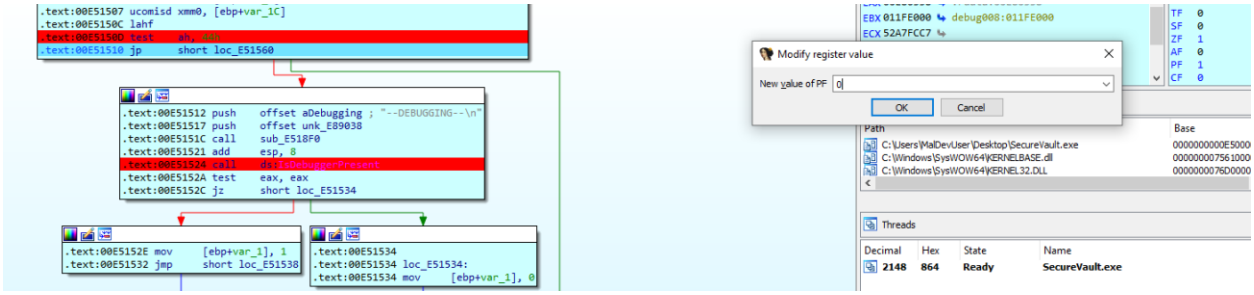
and need help to find a way into the vault. Can you help us?

Task:

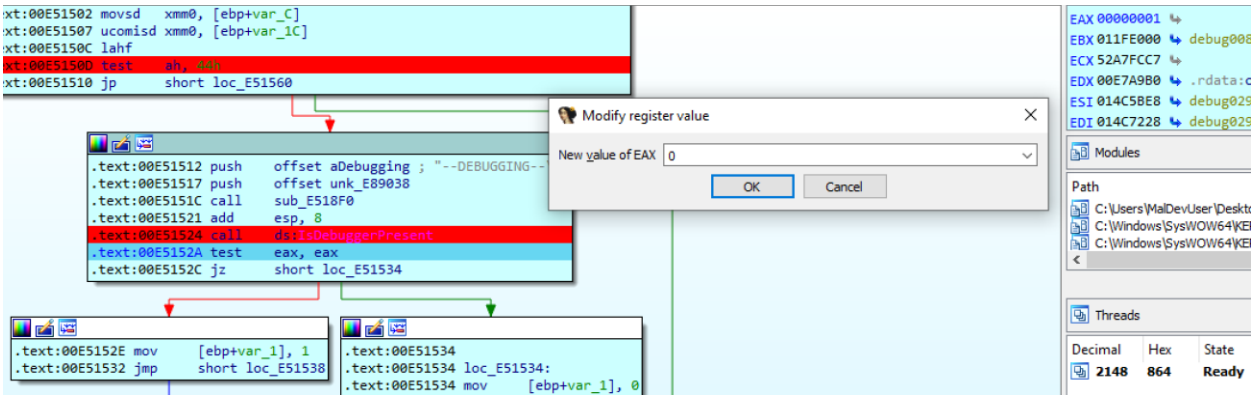
Find out what is inside thevault

---

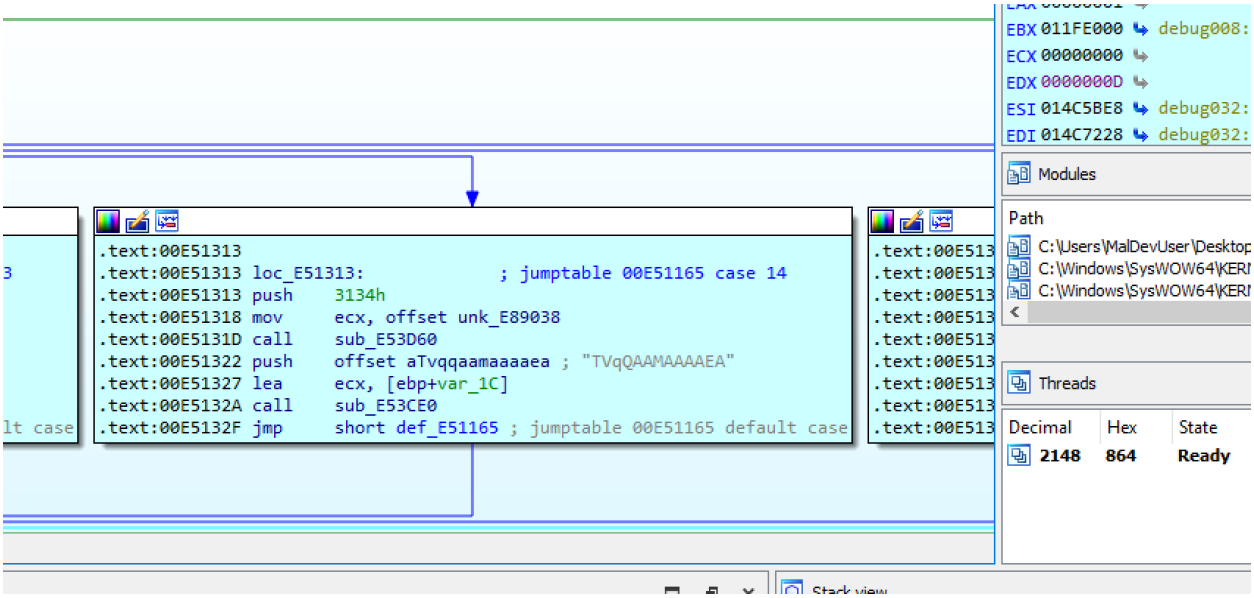
1. Simply checking the binary it looks like we want to end up on the left side where “IsDebuggerPresent” is located. By changing the register PF we can force the program to run the code on the left branch.



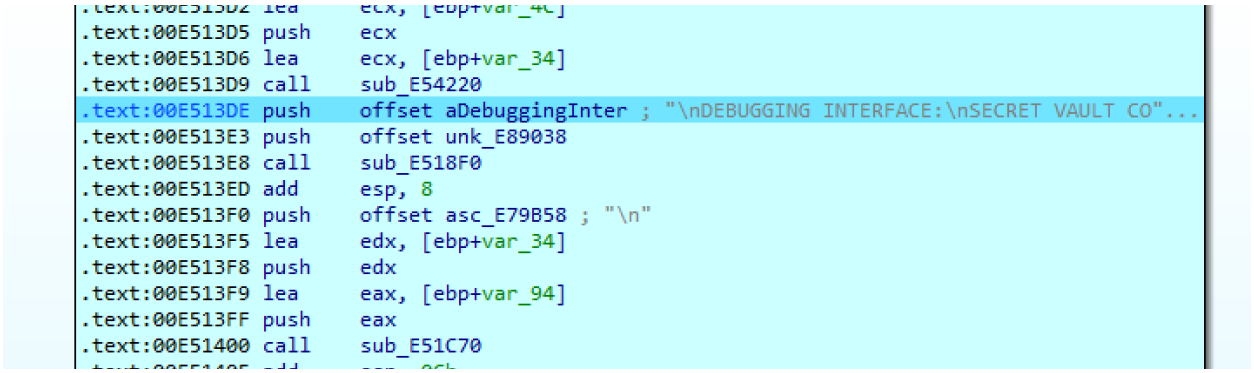
2. Next we want to get around the Debugger-Check by setting eax to 0



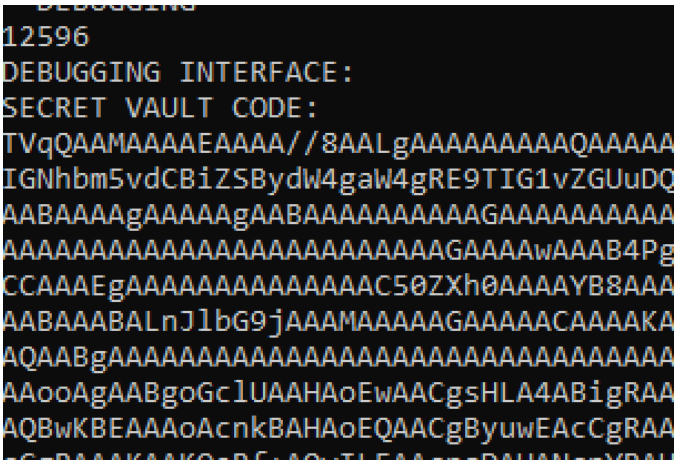
3. As we do not know which path is correct and will yield the flag we try just stepping trough without changing anything. We do that until we end up at a bigger switch-case. The text in the console mentioned the key 14 so we want to try to select case 14. We can control the outcome of the switch-case by setting exd to 0xd



4. Stepping trough the rest of the code we can see the string “DEBUGGING INTERFACE” this seems like something we want to check out.

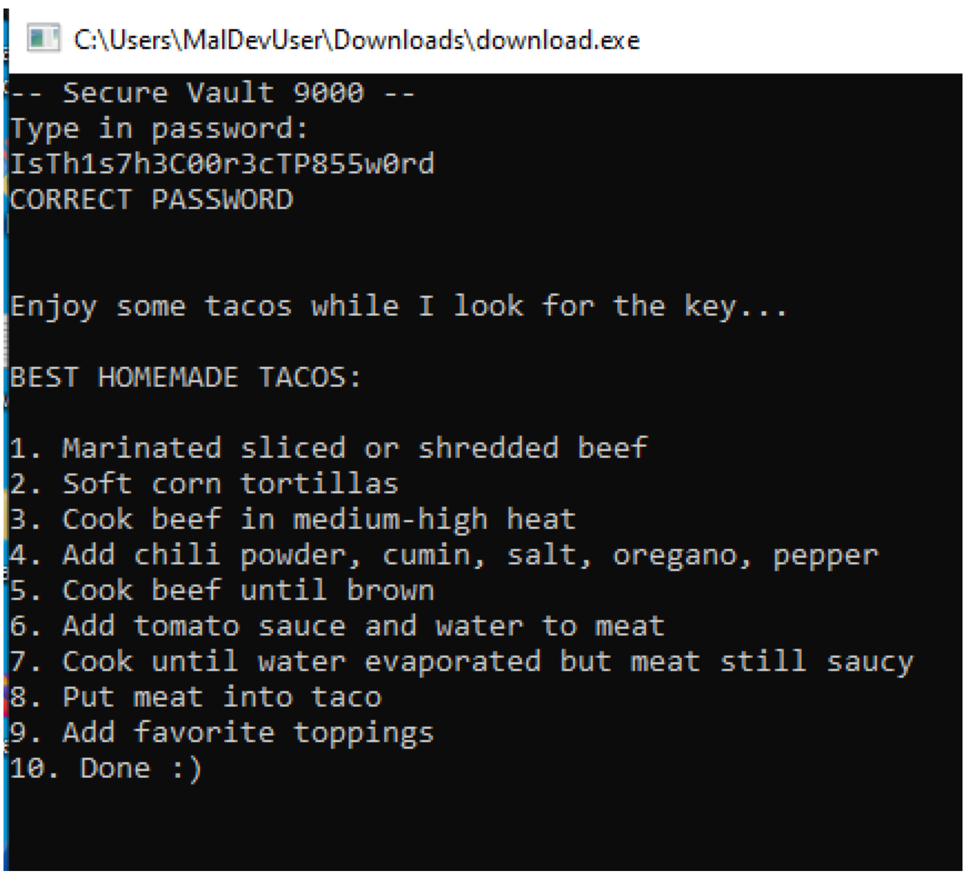


5. After a few calls this will print out a very long code as “SECRET VAULT CODE”

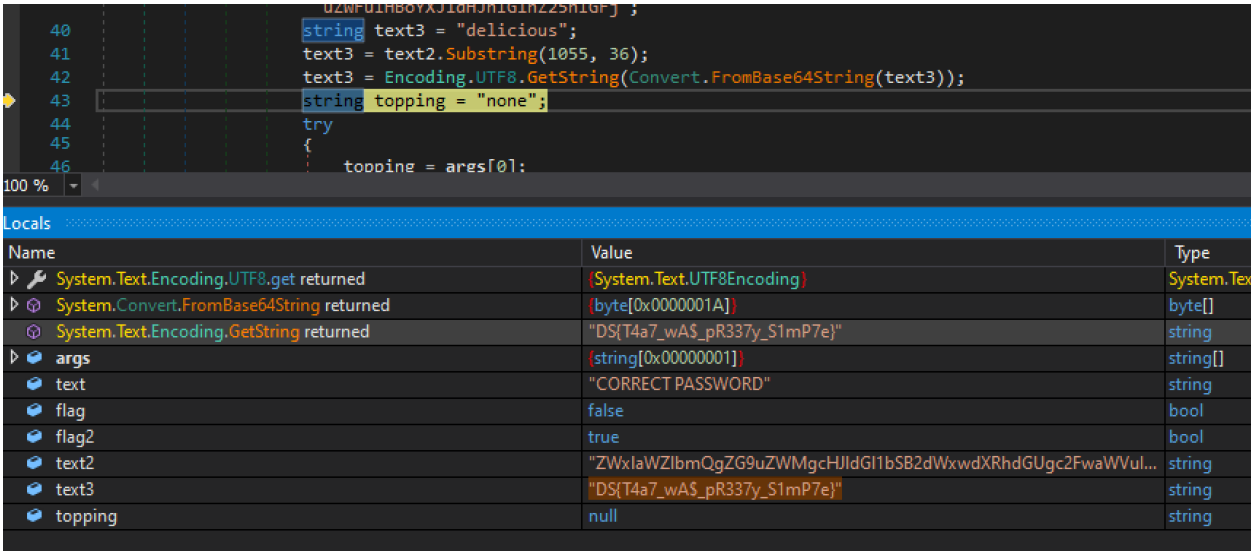


6. Looking at the code this could be base64-encoded
7. Seeing the MZ-header we can be sure that this is another binary so we copy the whole code and decode it and then save it as dump.exe

8. Checking the binary with DiE we can see that is a .NET-Binary
9. To debug .NET we can use dnSpy (32Bit in this case)
10. Simply stepping trough the binary we can figure out that the password for the binary is IsTh1s7h3C00r3cTP855w0rd



11. Stepping trough the code we get to a base64-decoded string. After decoding we can see the actual flag


40 string text3 = "delicious";
41 text3 = text2.Substring(1055, 36);
42 text3 = Encoding.UTF8.GetString(Convert.FromBase64String(text3));
43 string topping = "none";
44 try
45 {
100 %
Locals
Name
Value
Type
System.Text.Encoding.UTF8.get returned
{System.Text.UTF8Encoding}
System.Convert.FromBase64String returned
{byte[0x0000001A]}
byte[]
System.Text.Encoding.GetString returned
"DS{T4a7_wA$_pR337y_S1mP7e}"
string
args
{string[0x00000001]}
string[]
text
"CORRECT PASSWORD"
string
flag
false
bool
flag2
true
bool
text2
"ZWxlaWZlbmQgZG9uZWMgcHJldGl1bSB2dWxwdXRhdGUgc2FwaWVul...
string
text3
"DS{T4a7_wA$_pR337y_S1mP7e}"
string
topping
null
string