**Dead Drop**

***Programming***

**Challenge:**

The Incident Response Team at Aurora Pharmaceuticals recently recovered this file from a user’s computer. The artifacts indicate it was accessed by what they believe to be multiple DEADFACE members. The program appears to have set up the user’s workstation as a dead drop for DEADFACE members to convert a secret numerical code into a password string for further target access. Our decoding attempts have been unsuccessful, but the script appears to contain a recovery code that may be a good starting point.

Submit the flag as flag{the password} exactly how print\_password() returns it.

Attached - deaddrop.py

**Approach:**

Not much of a rocket science actually.

There’s a function named left\_shift given in the python code and two commented out lines:

# Password recovery:

# buA9kvZ=T\_A}b[J8l:@ob\_tviPZtb\_<olOpxkvZ=T\_=xju]olOpxkvZ=T\_bxlu]olOpxkvZ=QIEE

Taking a guess, we create a small for loop from 0 to 50 and use the left\_shift function with this string above and the number:

s = "buA9kvZ=T\_A}b[J8l:@ob\_tviPZtb\_<olOpxkvZ=T\_=xju]olOpxkvZ=T\_bxlu]olOpxkvZ=QIEE"

for i in range(50):

print(left\_shift(s,i))

We notice there are a lot of gibberish strings, but upon looking closely we see a string:

Zm91cnR5LW9uZSB0d28gZWlnaHRlZW4gdGhpcnR5LW5pbmUgdGhpcnR5LWZpdmUgdGhpcnR5IA==

Now, there are chances people might skip it because it looks gibberish, but to me it looks like its encoded (probably base64 because of the = sign at the end?)

We check and we were right and decode it to:

fourty-one two eighteen thirty-nine thirty-five thirty

Now, there’s an array given in the python program named by ‘arr’ and another function named ‘print\_password’ which takes a parameter of a integer array and traverse through the main array only on the integers given in the num array, create a string out of those values and print it.

We convert the decoded result wee got above into numbers:

41, 2, 18, 39, 35, 30

Maybe this is the num array?

num = [41, 2, 18, 39, 35, 30 ]

We run the function and got the flag as output:

**Flag: flag{the current plan is world domination}**

Congrats!!

Happy Hacking!