Logon Zero

נתון שרת עם כמה אופציות.

Authenticate – משווה את הסיסמא שאנחנו מעבירים לסיסמא של השרת, מדפיס דגל אם צדקנו

Reset_connection – יוצר cipher חדש עם מפתח רנדומלי

Reset_password – מקבל token משלנו באורך 28 בתים לפחות. מבנה הטוקן הוא כזה:

Encrypted Password	?
Password Length	4

בפועל 16 הבתים הראשונים משמשים לIV ולכן האורך המינימלי של סיסמא חייב להיות 8 (28 בתים בכולל פחות 16 לIV ו4 לאורך)

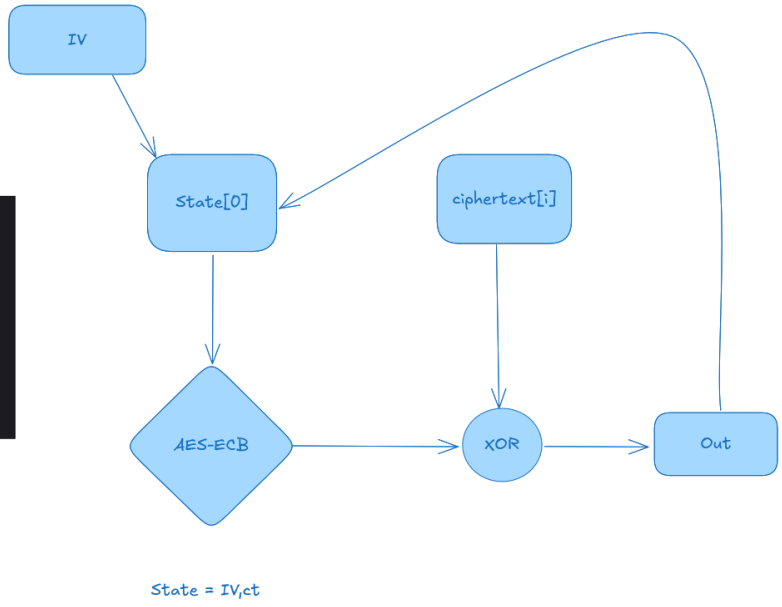
לבסוף הסיסמא תהיה decrypt(token)[:pass_len]

הדבר הראשון שעלה לי לראש זה לנסות לגרום לpassword length להיות מאוד נמוך בreset password

כלומר ש4 הבתים האחרונים יהיו קטנים או שווים ל3.

נבין איך decrypt עובדת:

```
def decrypt(self, ciphertext):
    IV = ciphertext[:16]
    ct = ciphertext[16:]
    cipher = AES.new(self.key, AES.MODE_ECB)
    pt = b''
    state = IV
    for i in range(len(ct)):
        b = cipher.encrypt(state)[0]
        c = b ^ ct[i]
        pt += bytes([c])
        state = state[1:] + bytes([ct[i]])
    return pt
```



אוקיי – מעניין!

בתכלס, דרך אחת לנצח היא להשיג את הform encrypted של כל דבר, כלומר צמד plaintext-ciphertext

במקרה כזה נוכל להכניס את הtoken הבא:

$$P, C$$

Decrypt על זה יבצע:

$$pt = E(P)[i] \oplus C[i] = 0$$

אבל אין לנו את זה כי אין לנו דרך להדליף כלום מהשרת

מה אם פשוט נשלח המון אפסים? כלומר טוקן שמכיל 28 בתים שערכם 0?

יתבצע בדיוק : $pt[i] = E(0)[0] \oplus 0 = E(0)[0]$

אז אנקדוטה מעניינת זה שעם FF כן יוצא בערך פעמיים-שלוש בכל 500 ניסיונות שאורך הסיסמא הוא 0

```
75
76  challenge = Challenge()
77
78  i = 0
79  while i < 500:
80      challenge.challenge({"option": "reset_password", "token": "FF"*28})
81      if challenge.password_length < 8:
82          print(challenge.password)
83      i += 1
84      challenge.challenge({"option": "reset_connection"})
85
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 1

```
[05:40 PM]-[liam@liampc]-[~/.../cryptohack/Stream_Ciphers]- |main ✓|
$ python3 logon_zero.py
b''
b''
b''

[05:40 PM]-[liam@liampc]-[~/.../cryptohack/Stream_Ciphers]- |main ✓|
$
```

לא לגמרי ברור לי למה אבל זה כן הגיוני שלרסט את המפתח הרבה ולשלוח טוקן קבוע ישגע את השדה של אורך הסיסמא שנגזר מהפענוח של הטוקן

מפה לשם קצת ריסטים ויש פלאג!

```
$ python3 logon_zero.py
Please authenticate to this Domain Controller to proceed

{"msg": "Welcome admin, flag: crypto{Zerologon_Windows_CVE-2020-1472}"}
```