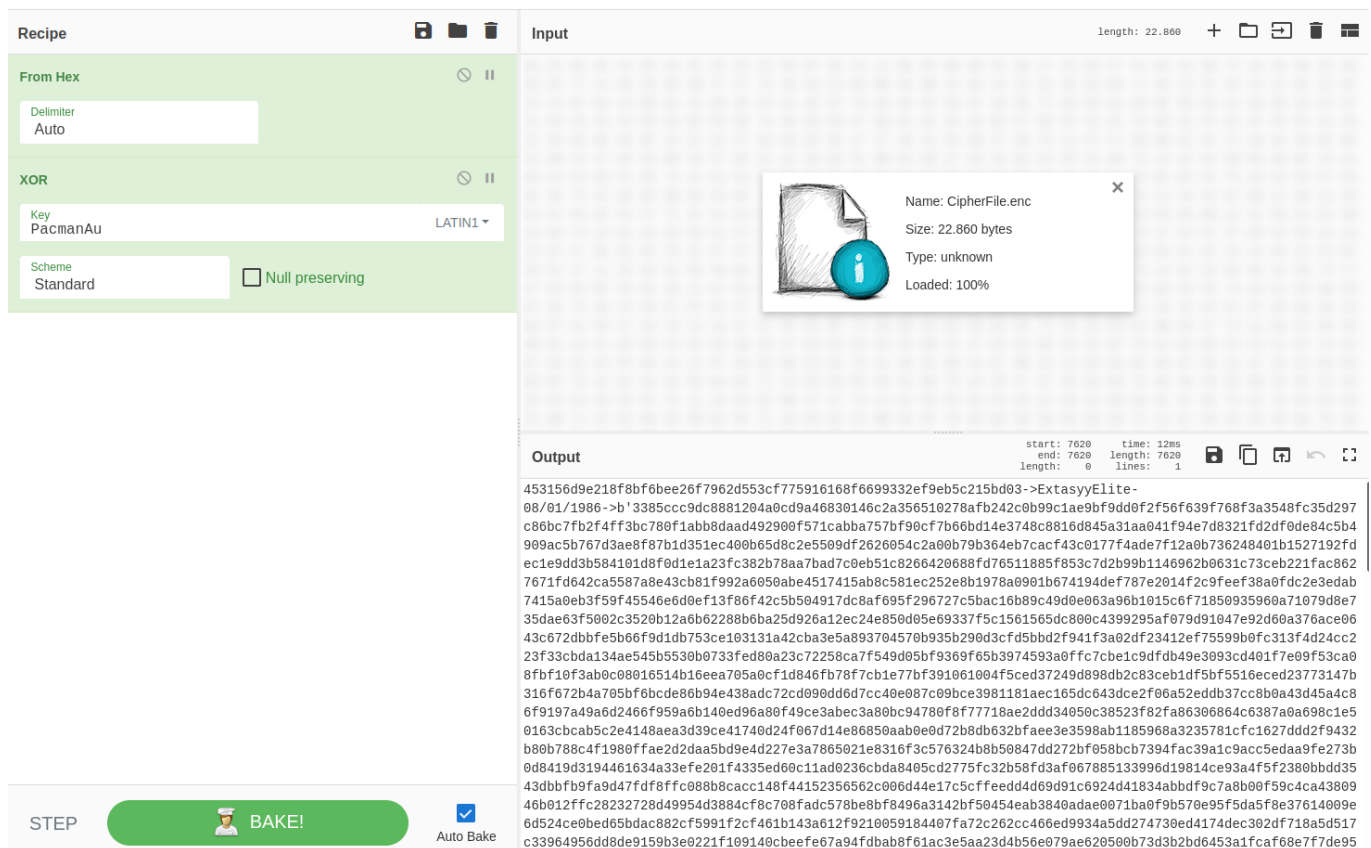


Autores: DiegoAltF4, Dbd4

Se puede ver que hay una función que cifra "aes_encrypt". Esta función cifra usando AES y luego llama a la función "write_file" que concatena una serie de variables al cifrado en AES, le aplica un XOR y lo escribe a un fichero "Cipherfile.enc".

Este fichero es el que se nos proporciona junto con el .py. Hay que saber que el XOR devuelve la información en hex, por lo que el primer paso será decodificarlo. Además, tenemos que darnos cuenta de que la función XOR está empleando una key ("PacmanAularioTres"), pero solo se está usando una parte de esta key, que se especifica como argumento al llamar al programa ("-x"). Por tanto, como no sabemos esta longitud, podemos introducir toda la key e ir eliminando caracteres desde el final al principio hasta que salga algo con sentido. La longitud indicada era 8 por lo que, al introducir como key PacmanAu se debería poder visualizar la siguiente información:



Con el resultado obtenido podemos ver: el identificador, grupo, fecha y la información cifrada en AES.

Tanto el identificador como la key dependen de una variable r. Sabiendo el identificador se puede hacer fuerza bruta para encontrar la r correcta y por tanto, generar la key empleada para cifrar. Esta key es la que nos va a permitir descifrar la información.

En este caso, tras hacer fuerza bruta de la r, el resultado obtenido es 3894. Ya tenemos todos los datos para descifrar el AES.

El script final es:

```
import argparse, random, os
import pyaes, rsa, hashlib
from pwn import *
GROUP = 'ExtasyElite'
DATE = '08/01/1986'

def get_args():
    parser = argparse.ArgumentParser(description='BestCipher v1.1')
    parser.add_argument('-i', '--id', type=str, help='Known identifier',
                        required=True)
    parser.add_argument('-f', '--file', type=str, help='Encrypted hex data',
                        required=True)
    args = parser.parse_args()
    return (args.id, args.file)

def get_data(file):
    with open(file, 'r') as fp:
        data = fp.read()
    return data

def get_random_aes_key(size, length=32):
    random.seed(GROUP)
    for i in range(size):
        random.getrandbits(8)
    else:
        key = bytearray((random.getrandbits(8) for x in range(length)))
    return key

def aes_decrypt(data, key):
    data = bytes.fromhex(data)
    aes = pyaes.AESModeOfOperationCTR(key)
    encdata = aes.decrypt(data)
    print(encdata)
    write('solucion.dec', encdata)

def crack_r(size, known_id):
    for r in range(16384): # 2^14
        identifier = '{}|{}|{}|{}'.format(GROUP, DATE, str(size), str(r))
```

```

        result = hashlib.sha256(identifier.encode())
        hash = result.hexdigest()
        if(hash==known_id):
            return r
    print("No se ha encontrado un r correcto")
    return 0

if __name__ == '__main__':
    known_id, file = get_args()
    hexData = get_data(file)
    size = int(len(hexData)/2) #cada byte son dos numeros hex
    r = crack_r(size,known_id)
    print("La r bruteforceada es: "+str(r))
    aeskey = get_random_aes_key(size + r)
    aes_decrypt(hexData,aeskey)

```

El uso del script es:

```

python3 solver.py -i
453156d9e218f8bf6bee26f7962d553cf775916168f6699332ef9eb5c215bd03 -f aes.txt

```

Si ahora miramos el contenido del fichero "solucion.dec" podremos ver el texto en claro que se cifró usando AES y por tanto la ansiada flag:

```

=====
The following was written shortly after my arrest...

        /\The Conscience of a Hacker\/

                by

                +++The Mentor+++

                Written on January 8, 1986

=====

        Another one got caught today, it's all over the papers. "Teenager
Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...
        Damn kids. They're all alike.

        But did you, in your three-piece psychology and 1950's technobrain,

```

ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."

Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...

Or feels threatened by me...

Or thinks I'm a smart ass...

Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. HackOn{3L_M4n1F135T0_H4ck3r_es_mi_unica_novela}

"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color,

without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

Flag: `HackOn{3l_M4n1F135T0_H4ck3r_es_mi_unica_novela}`