WriteUp Final JOINTS2021
Brahmastra

Tribun Network
Tribun Timur
SEORANG SUPIR PROTES DIBERHENTIKAN MEMBUAT
SEJUMLAH PETUGAS DISHUB KABUR TINGGALKAN LOKASI

TEMPE GEMBUS

Seorang Supir Protes Diberhentikan Membuat Sejumlah Petugas Dishub Kabur Tinggalkan Lokasi

MBEERRR
ChaO
AnehMan

Cryptography

1. Here We AES Again

a. Executive Summary

We are bored and decide to try this mode of AES to be used for our secret agent service. Please test it out.

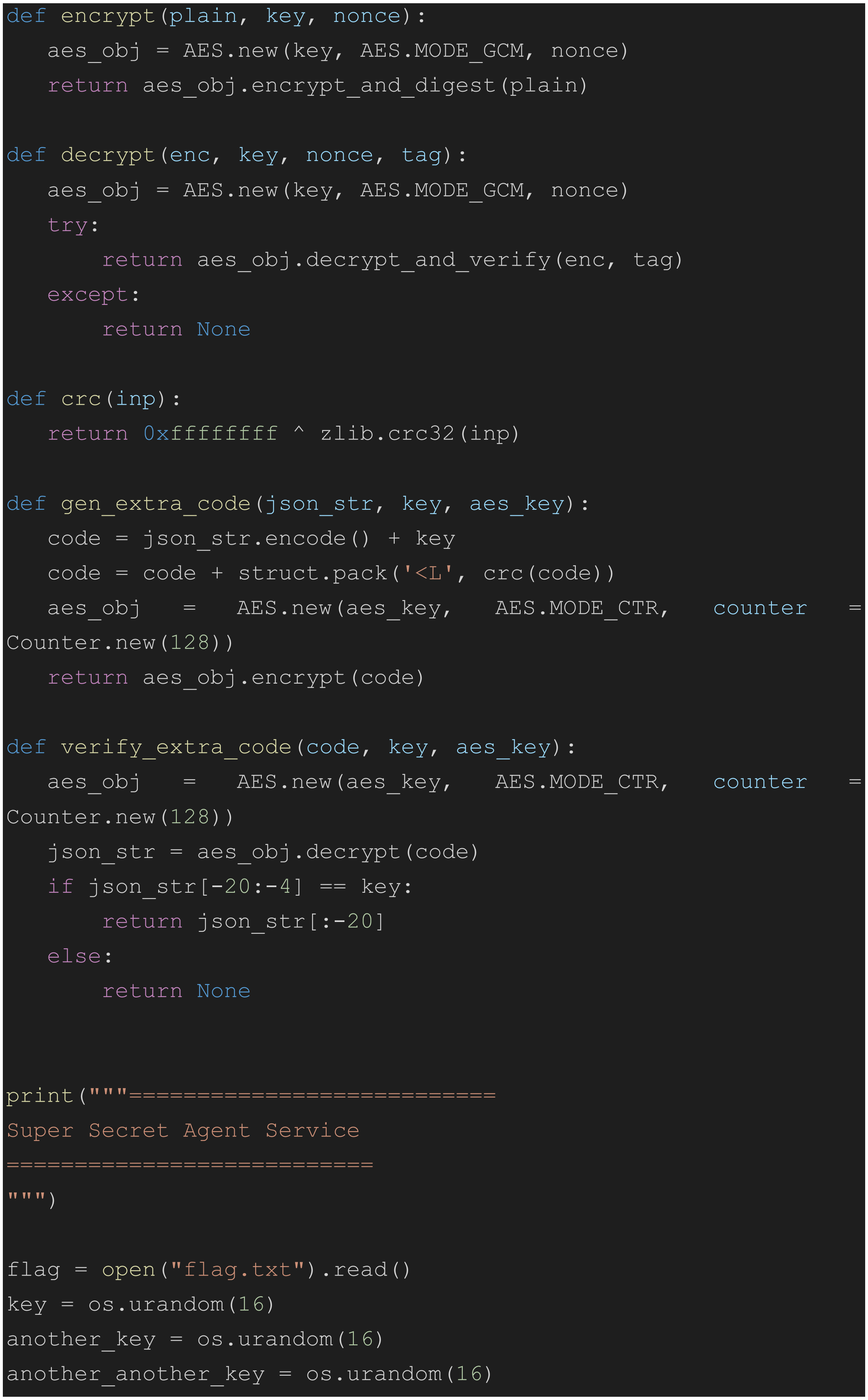
nc dubwewsub.joints.id 20001

Author : yeraisci

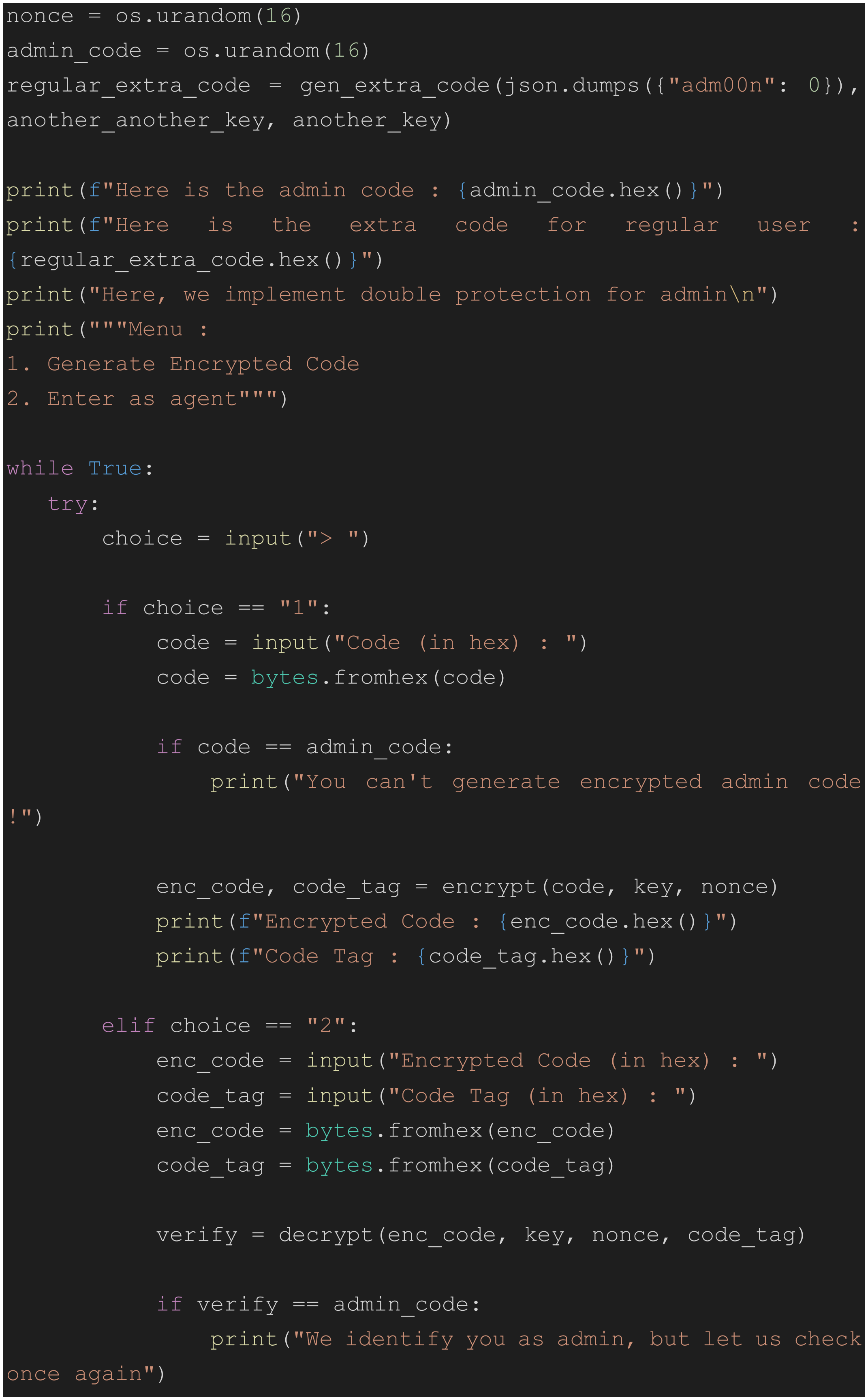
b. Technical Report

Diberikan file chall.py, berikut penampakannya.

```python
#!/usr/bin/env python3

from Crypto.Cipher import AES
from Crypto.Util import Counter
import os
import struct
import json
import zlib
import sys

class Unbuffered(object):
  def __init__(self, stream):
      self.stream = stream
  def write(self, data):
      self.stream.write(data)
      self.stream.flush()
  def writelines(self, datas):
      self.stream.writelines(datas)
      self.stream.flush()
  def __getattr__(self, attr):
      return getattr(self.stream, attr)

sys.stdout = Unbuffered(sys.stdout)
```



```python
def encrypt(plain, key, nonce):
    aes_obj = AES.new(key, AES.MODE_GCM, nonce)
    return aes_obj.encrypt_and_digest(plain)

def decrypt(enc, key, nonce, tag):
    aes_obj = AES.new(key, AES.MODE_GCM, nonce)
    try:
        return aes_obj.decrypt_and_verify(enc, tag)
    except:
        return None

def crc(inp):
    return 0xffffffff ^ zlib.crc32(inp)

def gen_extra_code(json_str, key, aes_key):
    code = json_str.encode() + key
    code = code + struct.pack('<L', crc(code))
    aes_obj = AES.new(aes_key, AES.MODE_CTR, counter = Counter.new(128))
    return aes_obj.encrypt(code)

def verify_extra_code(code, key, aes_key):
    aes_obj = AES.new(aes_key, AES.MODE_CTR, counter = Counter.new(128))
    json_str = aes_obj.decrypt(code)
    if json_str[-20:-4] == key:
        return json_str[:-20]
    else:
        return None


print("""===========================
Super Secret Agent Service
===========================
""")

flag = open("flag.txt").read()
key = os.urandom(16)
another_key = os.urandom(16)
another_another_key = os.urandom(16)
```



```python
nonce = os.urandom(16)
admin_code = os.urandom(16)
regular_extra_code = gen_extra_code(json.dumps({"adm00n": 0}), another_another_key, another_key)

print(f"Here is the admin code : {admin_code.hex()}")
print(f"Here is the extra code for regular user : {regular_extra_code.hex()}")
print("Here, we implement double protection for admin\n")
print("""Menu :
1. Generate Encrypted Code
2. Enter as agent""")

while True:
    try:
        choice = input("> ")

        if choice == "1":
            code = input("Code (in hex) : ")
            code = bytes.fromhex(code)

            if code == admin_code:
                print("You can't generate encrypted admin code !")

            enc_code, code_tag = encrypt(code, key, nonce)
            print(f"Encrypted Code : {enc_code.hex()}")
            print(f"Code Tag : {code_tag.hex()}")

        elif choice == "2":
            enc_code = input("Encrypted Code (in hex) : ")
            code_tag = input("Code Tag (in hex) : ")
            enc_code = bytes.fromhex(enc_code)
            code_tag = bytes.fromhex(code_tag)

            verify = decrypt(enc_code, key, nonce, code_tag)

            if verify == admin_code:
                print("We identify you as admin, but let us check once again")
                extra_code = input("Enter Extra Code : ")
                extra_code = bytes.fromhex(extra_code)
                admin_json = json.loads(verify_extra_code(extra_code, another_another_key, another_key))

                if admin_json["adm00n"]:
                    print(f"Welcome admin, here is your flag : {flag}")
                    exit()
                else:
                    print("Unfortunate, your extra code is wrong")

            else:
                print("Welcome agent, have fun here :)")

        else:
            print("Invalid Choice !")

    except:
        print("Something Error !")
```

Ada beberapa hal yang perlu diperhatikan:

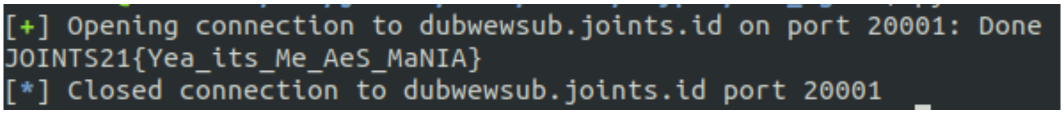
1. Ketika generate encrypted code, ada pengecekan kalau inputan sama dengan admin code, tampilkan pesan kalau kita tidak bisa generate code. Tapi bukannya break atau ada kolom else, malah langsung lanjut. Jadinya kita bisa generate code untuk admin
2. Ketika generate extra code, json adm00n di concat dengan key + crc(json adm00n + key). Tetapi ketika proses verify, crc tidak dicek. Jadi kita bisa melakukan bit-flip agar value adm00n yang sebelumnya 0 menjadi 1. Hal ini bisa dilakukan karena AES CTR adalah stream cipher (plaintext ^ keystream = ciphertext)
3. Ketika sudah memasukkan extra code yang sudah diubah, flag di print. Tapi setelah di print, muncul spam “Something Error !”. Jadi kita harus mengambil flagnya dengan recvline (pwntools)

Berikut adalah full scriptnya

```
from pwn import *
from binascii import unhexlify, hexlify
```

```
# p = process("./chall.py")
p = remote("dubwewsub.joints.id", 20001)

# mengambil admin_code dan extra_admin_code
p.recvuntil("Here is the admin code : ")
admin_code = p.recvline().strip()
p.recvuntil("Here is the extra code for regular user : ")
extra_user_code = unhexlify(p.recvline().strip())

# generate enc_code dan code_tag untuk admin
p.sendline("1")
p.sendline(admin_code)
p.recvuntil("Encrypted Code : ")
enc_code = p.recvline().strip()
p.recvuntil("Code Tag : ")
code_tag = p.recvline().strip()

# send enc_code dan code_tag adm00n
p.sendline("2")
p.sendline(enc_code)
p.sendline(code_tag)

# bit-flip
not_adm00n = '{"adm00n": 0}'
adm00n = '{"adm00n": 1}'
payload = xor(not_adm00n,adm00n)
tampered = xor(extra_user_code[:len(payload)],payload) +
extra_user_code[len(payload):]
tampered = hexlify(tampered)
p.sendline(tampered)

# recvline flag
p.recvuntil("Welcome admin, here is your flag : ")
print(p.recvline().strip().decode())
```

Hasil:



```
[+] Opening connection to dubwewsub.joints.id on port 20001: Done
JOINTS21{Yea_its_Me_AeS_MaNIA}
[*] Closed connection to dubwewsub.joints.id port 20001
```

c. Flag

Flag: **JOINTS21{Yea_its_Me_AeS_MaNIA}**

Free Flag

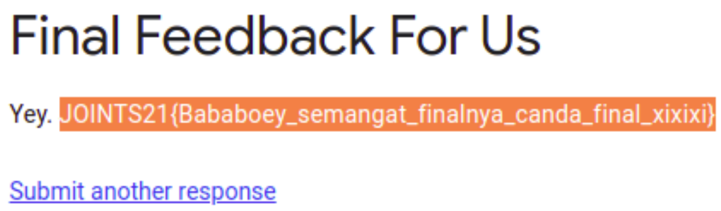
1. Enade Fri Flek

a. Executive Summary

Another free flag. Really appreciated bro 👊 https://forms.gle/6UtEzaMHFP64DEs57

b. Technical Report

Isi sepenuh hati, dapet flag….



Final Feedback For Us

Yey. JOINTS21{Bababoey_semangat_finalnya_canda_final_xixixi}

c. Flag

Flag: **JOINTS21{Bababoey_semangat_finalnya_canda_final_xixixi}**