永信至诚春秋Game CTF赛题设计说明

[题目信息]:

出题人	出题时间	题目名字	题目类型	难度等级	题目分值
Soreat_u	20210510	logon	crypto	5	300

[题目描述]:

```
Here's a peculiar logon protocol. Can you break it?
```

[题目考点]:

```
1. AES加密模式
2. 登录协议
```

[是否原创]:

```
原创
```

[Flag]:

`flag{87c29cba-b142-11eb-8529-0242ac130003}`

[题目环境]:

```
docker
```

[特别注意]:

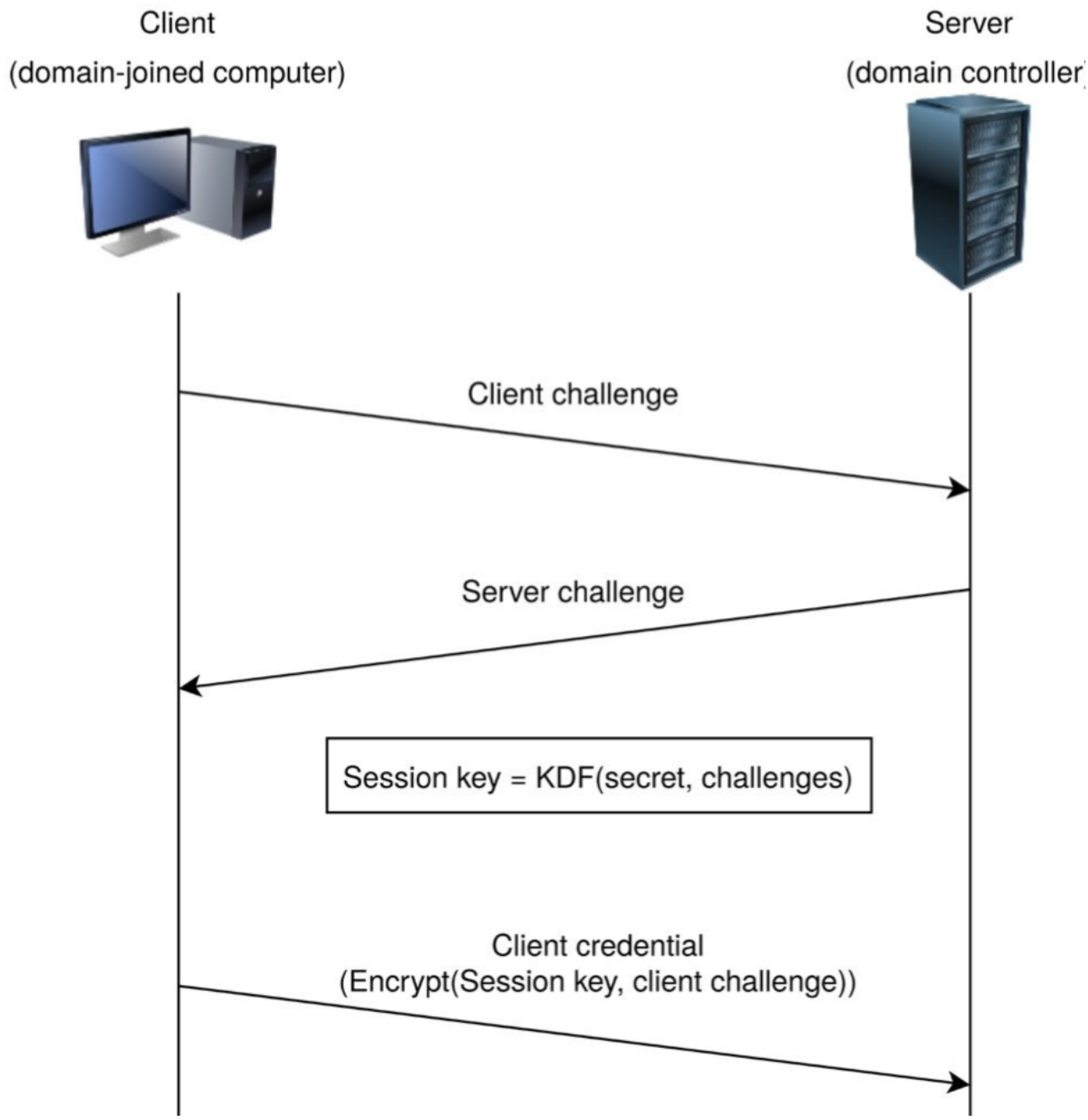
```
无
```

[题目制作过程]:

```
cd ./源码
docker build . -t crypto-logon
docker run --name crypto-logon -d -p 9999:9999 crypto-logon
```

[题目writeup]：

1. 简单审计，发现给了一个菜单，有登陆和注册两个功能，如果能够以Administrator用户登陆则可以getflag
2. 登陆协议如下图所示：



client先给server发送一个client challenge并提供登录的用户名，随后server检查用户名是否已注册，若已注册则返回一个server challenge。

client此时可以需要自己的密码（secret）和client challenge、server challenge计算出session key，并用session key对client challenge加密，将密文（client credential）发送给server。

server收到client credential后，用相同的方式根据本地数据库中存储的该用户对应的secret计算出credential，并与client credential对比，若一致，则证明client一定知道该用户的密码，从而登陆成功。

3. 问题出现在计算client credential的encrypt函数，此函数使用AES-CFB8模式进行加密，且IV默认为16个0字节。

   AES-CFB8模式加密过程如下图所示：

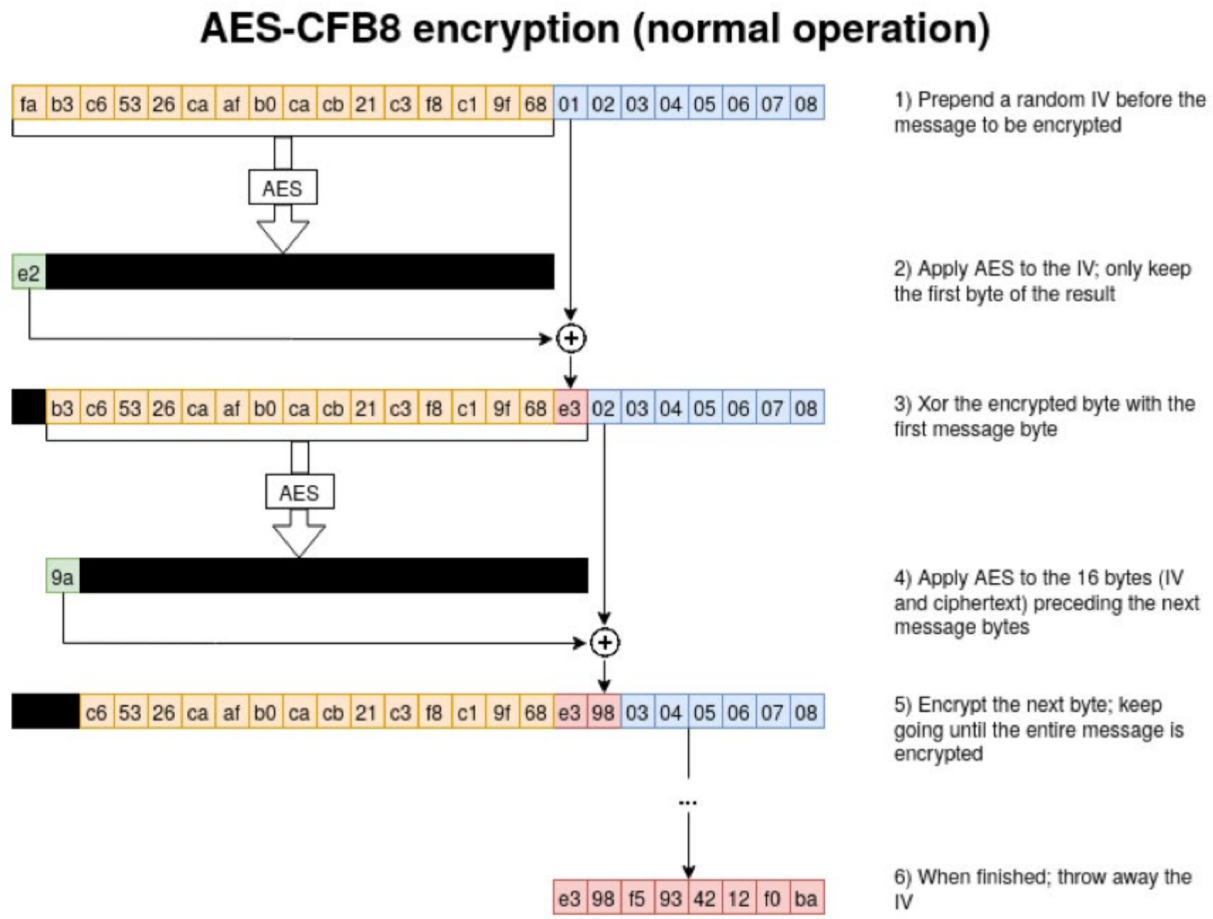


Figure 2: An illustration of encryption with the AES-CFB8 mode of operation.

该模式存在一个弊端：若IV全0且后面8字节的明文也都是0的话，那么密文有1/256的概率也全都是0

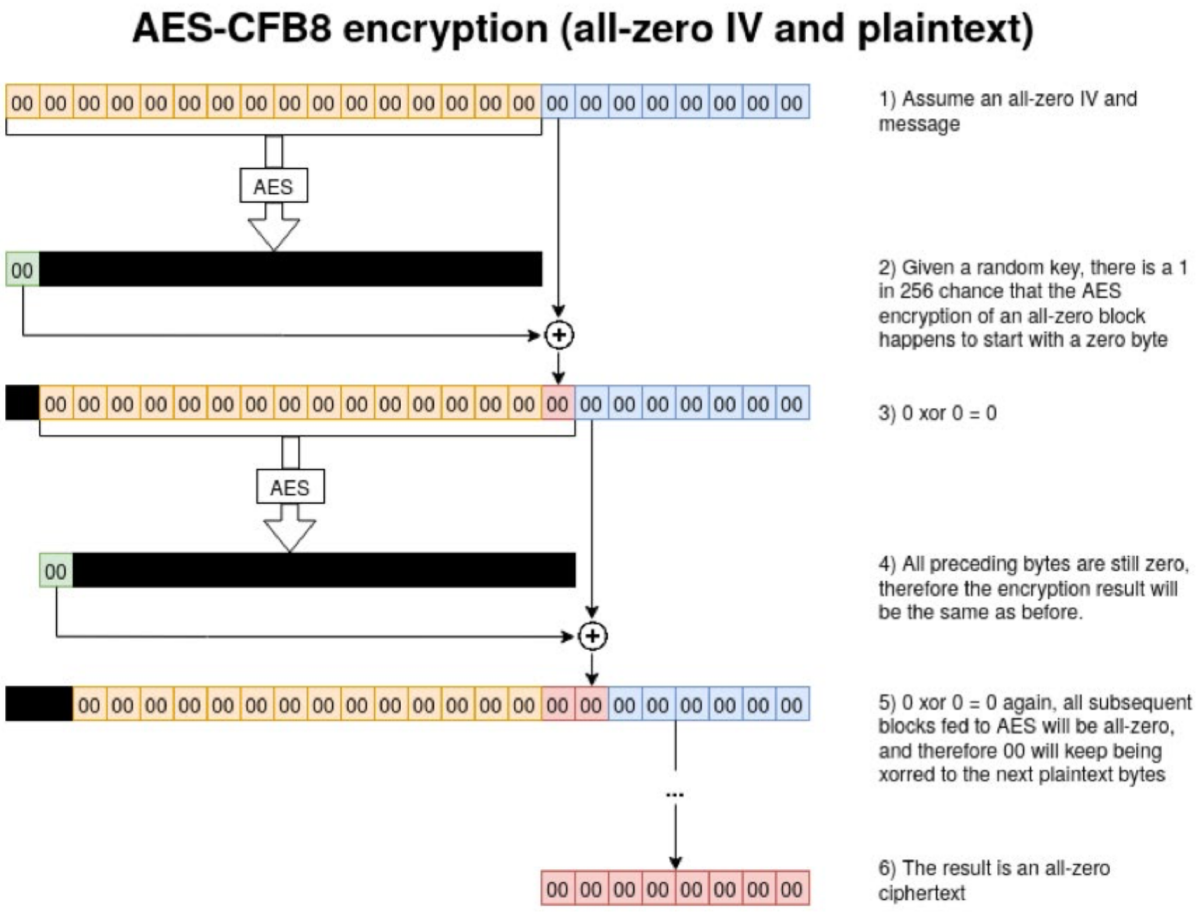


Figure 3: When encrypting a message consisting only of zeroes, with an all-zero IV, there is a 1 in 256 chance that the output will only contain zeroes as well.

4. 利用AES-CFB8模式的漏洞，可以发送client challenge全为0，username为Administrator，且client credential全为0，有1/256的概率可以通过check，getflag。
5. exp如下：

```python
from pwn import *

HOST = ""
PORT = 9999
conn = remote(HOST, PORT)

for _ in range(0x1337):
    conn.sendlineafter(b"> ", b"1")

    conn.sendlineafter(b"client challenge: ", b"0"*16)
    conn.sendlineafter(b"username: ", b"Administrator")
    conn.sendlineafter(b"client credential: ", b"0"*16)
    recv = conn.recvline()
    if recv != b"Login failed!\n":
        print(conn.recvline())
        conn.sendlineafter(b"> ", b"3")
```

```
        break

conn.close()
```