Orange CTF - Break The Bank

Scenario

After several months of tracking, Interpol has managed to locate and break into the security system of a bank used by a criminal organization. We are looking for the best students from your school for this new edition of our serious game "Capture the Flag": mission Break the Bank.

.... Good luck!

Before starting

- We have to connect with ssh to the remote server where all the files are available to solves challenges
- User, password and remote ip server are sent to the participants in an e-mail.
- All flag are like : `{CHALLENGE_NAMEXX:BASE64ENCODED}`

Starter

START01 - Oh my Host !!!

10 points

Get hosts on the remote machine

`cat /etc/hosts`

`FLAG : {STARTER01:d2hhdCBhIHVzZWZ1bGwgZmlsZQ==}`

START02 - Very Nice Challenge

10 points

TO COMPLETE

START03 - Find me

10 points

The flag is the only city where it is not in Casa De Papel show

`FLAG : {STARTER03:Milano}`

Banking

We wanted to get a graphical interface of the website instead of a CLI one, we needed to tunnel the ssh connection to a port without a specific endpoint (`port 9050` in our case) :

1. We connect from remote and open a port `ssh -D 9050 kali@[ip]` where `ip` is told to us with the CTF email
2. Using the `nestat -tn` we access to all hosted servers and their port
3. The bank website is hosted at `10.0.0.14:80`
4. Add a proxy to our browsers in `SOCKS Host` section : `127.0.0.1` and port `9050`.
5. Now if we go to `10.0.0.14:80`, we can navigate through the bank website.

Most of the challenges were resolved by using the endpoint `10.0.0.14:80/robots.txt`

BANK01 - what a style!

50 points

The name of the challenge is surely linked with the style (`css`) of the webpage, we searched on each `css` files.

Then we finally have interesting thing in `main.css`, a property containing `RkxBR3tCQU5LSU5HMTpjbVZoWkhSb1pXTWtKQT09fQ==` which is the flag encoded in base64

Decoded message : `FLAG :{BANKING1:cmVhZHRoZWMkJA==}`

`cmVhZHRoZWMkJA==` decoded in base64 : `readthec$$`

BANK02 - Hodor's account

100 points

A sql file is available at the endpoint /sql/data.sql, we have a sql script with password encrypted for Hodor.

His password seems to be not encrypted (`'HODOR!? Hodor? HODOR? hodor. hodor? rHoO | odoOorHODOR Hodor Hodor... oHodor. Hodor? HODOR? hodor!'`) but it is, we decrypted using Hodor algorithm. It gives us `winterIsComing` which is his password, his username is `hhodor` When logging in, if we go down to the transaction page, we got the flag :

`FLAG: {BANKING2:aG9kb3Job2RvcmhvZG9yNTE=}`

`aG9kb3Job2RvcmhvZG9yNTE=` decoded in base64 : `hodorhodorhodor51`

BANK03 - It's christmas ! (partially resolved)

200 points

Using the endpoint `/secret/secrets.txt`

We find the following text : `// AES/ECB-EDE/NO-Padding` `I1Arxhucf7RooXyRNrgtzUfm/LcaG4vxWRktZhuxbyqsuziMuCuamDASms3u1vsT` This message is encoded with AES' algorithm and we have to decipher it in 3 step, decode / encode / decode.

BANK04 - Common business oriented language

100 points

From the website we can obtain a file from `/robots.txt` which is `intellectual-property.cbl` a cobol script.

We use an online compiler to execute the code : https://www.tutorialspoint.com/compile_cobol_online.php but there is a syntax error on line 2, we need to add a `.` (dot) at the end of the line after 'CTF'. we get :

```
>FlaG:                                               <
>RkxBR3tCQU5LSU5HNDpRekJDTUV4cEpFRjNaWE52YldVaElRPT19<
```

Decoded in base64 : `FLAG : {BANKING4:QzBCMExpJEF3ZXNvbWUhIQ==}`

where `QzBCMExpJEF3ZXNvbWUhIQ==` decoded in base64 is `C0B0Li$Awesome!!`

BANK05 - Google Is My Friend

50 points

Getting on the website, we look around the source code.

At the bottom of it we get this comment :

```
<!-- We could have added https://letmegooglethat.com/?
q=CT%46%20%46%4CAG%7BB%41NK%49NG5%3AZmVsaXogbmF2aWRhZA%3D%3D%7D in order to be
more social -->
```

We go on the link and it shows the flag

`FLAG : {BANKING5:ZmVsaXogbmF2aWRhZA==}`

`ZmVsaXogbmF2aWRhZA==` decoded in base64 : `feliz navidad` which means "merry christmas" in spanish.

Android

Android01 - MyLittlePony

50 points

Find the right folder of a android application project using `adb`

TO COMPLETE