CTF – Creation

The begging:

When I got the assignment to so the ctf I was really worried, because I've never done any ctf, and I had no idea what to do or how to start it. And evidently so I did a lot of mistakes, the main of which were two mistakes: 1- not prepare the whole thing, step by step in a document (as I was told to do), 2- To start and not finish. So, I ended up with having a folder in my desktop called "ramam" and in it, about 7 different version of ctfs I started, got really far but didn't finish writing. Maybe sometime in the future ill finish them, all have their unique story and tricks.

Introduction:

The story line:

I always loved movies, and we all know the importance and magnitude of the movie:" The Matrix", once in a while I would watch the movie to think again about the philosophical dilemma that movie presents. And a huge bonus is the whole computer themed story line. So, when I was told to create a CTF with a back story. I was immediately drawn to the "matrix" themed story.

One of the most impactful scenes of the movie is the "red pill – blue pill dilemma" - stay and wake in your bed, don't worry about the justice of the world. Or, work hard and fight for the correctness of the world, even if its full of danger, etc....

So, I decided to start my CTF on the idea of the decision that the participant must take.

The "Flag" in the CTF:

The flag in the CTf in a link to the: "The Protocols of the Elders of Zion", and for a couple of reasons: 1- it says "protocols", which makes me laugh because, that what we learned in the course, "Network protocols". 2- "Zion" – the last human city in the Matrix. 3- The whole wiki page makes me laugh.

Declaimer

"It's not meant to hurt or offend anyone, if so, I apologize, it's for comedic purposes*

The creation of the CTF:

I WILL EXPLAIN THE CREATION OF THE CTF, FROM THE END (THE FLAG), TO THE BEGGING OF THE CTF (STAGE 1)

Stage 5 (final one):

I've decided to put the link in a http server the request a password. Simple. The server requests a password and waits for a http-post response, if the answer is correct then it'll print the link. I've decided to make the password a simple: 4 number pin, that could be broken in a brute force algorithm. The problem is: the participant, has no idea that the password is only 4 numbers. So how will the participant know the definition of the password?

The code for the http server: **http_server.py.**

Stage 4:

To get the definition of the password, the participant will need to reveres engineer an exe file. The exe file, created in c++, which has antidebug measures, does the following:

1- It has an encrypted python code.
2- Asks for a password from the participant.
3- If the password is correct, it'll decrypt the encrypted python code and the crated a pyc (python compiled) from the decrypted code

The code that decrypts the python file and creates the pyc file and has the antibug: **oracle_test.cpp**

the python code to encrypt the python file: **PythonEncrypter.py**

Stage 3:

The pyc file they receive after breaking the exe file is a udp/ip client that send packets to a certain ip. The packets are questions/challenges the require to write a server for it. After all the challenges are answered correctly, the client will print the definition of the password of the http - server the holds the link to the flag.

The code that sends the challenges etc: **Netword.py.**

Stage 2:

To receive the exe file and the http server, the participant receives a zip folder, which is encrypted using "7zip". The participant will need to write a code will find the password for the locked zip folder.

The code that creates the txt file (with the key words and hint) and the locks zip file while putting inside the exe file and http server file: **create_zip_rabbit_hole.py.**

Stage 1:

The folder that is locked is in a zipped folder with a txt file with key words and hints for the algorithm of the locked zip file.

The zip folder is downloaded when the participant chooses to take the "red pill" in the site that I created using this: website creator.

If the participant decides to now take on himself the tole to break the matrix and find the protocols, taking the "blue pill". The site will load a YouTube video to motivate him to break find the protocols and break out of the "Matrix".