Prison Break

Team name: Cyberons

Team members:

- Ricardo Aranaga
- Chaitanya Sai Pothuraju
- Matthew Alvidrez
- Chitti Lakshmi Deepak D

Project description:

The project includes a multi-layered layer. Each layer will give you a clue to decode the next layer.

At layer 0, Encrypted message is given to the participant and this encrypted message is generated by converting the original message to binary and the binary string is again converted to random ASCII value, where 1 is converted to random odd ASCII value and 0 is converted to random even ASCII value.
Output: TCP Server credential information. HINT: server riddle answers, methods to receive and send answers to server.

At layer 1, Client connects to a server and the server transmits messages with a time delay (Timing covert channel). The time delays are the multiples of 0.1 (i.e.., 0.1, 0.2, 0.3 … 1.0). The odd values represent binary `1" and even values represent binary "'0". As an added security, the server will ask three random riddles for the students to answer. The students will have to add a way to receive and send server messages to answer them. After 3 incorrect answers, they will have to change their IP address.
Output: SSH server credential information. HINT: FTP server credentials and credential options.

At layer 2a, Client connects to SSH server in a jailed environment with limited bash commands (disable ".." or cd works on limited directories). Create a multitude of folders with fake ones implanted that have to be traversed to find the correct folder where a stegged audio file is hidden. The probability of finding the hidden file in the folder maze is very small. The user will have to FTP to the same server based on the previous layer Hints.
Realization: FTP server credential information (same server IP, reversed credentials).

At layer 2b, Client connects to the FTP server in a jailed environment. Create a multitude of files where a message is hidden in the file permissions. So, the client would have to use a program that deciphers a covert message in the file permissions of a list of files and folders (7-bit/10-bit).
Output: Path location to an audio file

At layer 3, The audio file is stegged in the normal and reverse order. If the client finds the audio file before getting the instructions on how to stegg it (reversed). It will have a stegged image in an uncommon interval and offset that will provide a hint that they might be working on the wrong file.
Output: "We are captives of our own identities, living in prisons of our own creation.You've escaped the prison. Good luck my friend."

BOM:
There is nothing that they shouldn't already have from the class because everything that we used should be gone over in class so as long as they followed along, they will be fine to complete the challenge.

Cyber Storm setup and deployment:

- One TCP server to run the timing covert channel on campus. Students connect through VPN.
- Another Server Run "./install.sh" to create all the necessary files, FTP server, SSH server, users with passwords, and jailed environments.

Student introduction:

Welcome prisoners to the Prison Break Challenge!!! There is a power outage in the prison, so this is your opportunity to escape!! You will have to solve different cybersecurity puzzles to make your way out of this prison.

GET READYYYY!! GO!!!!

The credentials for TCP server are encrypted using a new pattern/method by nerd jailer and to decrypt it many prisoners tried but failed.

Only 4 prison escapees got success in decoding it. One of them left a clue i.e.., each character represents either 0 or 1. Get least significant bits (LSB) in binary ASCII value of each character and combined value is the key to this Puzzle.

Encrypted Message:

yxq8J3kervdotcyF2nDMWKHiNVQBeZHZsh33d3NCDL8yJ848lqmNKqDegK9Bfm5oGjvGcsLOyCR
36tSNNJTnEXoZophyk2WpZ6iutvwFYvqfrrFhgY6y2iUsqPDm6KAcCmvJEdGdtDT6mqfGt2koAG
4xqwX7LFPT2YAXXw6KGab1Grmuu8j4E2Cqz41XesUnTGRz7AHpy4fk5nBOVwsAPL7LlvGXHDFFI
uHspN1IqlAuylzWrtbDVeK2Zr8aVy4Nl8bkTMHYtvsHRqDnCQ6lkKbwcdfTIDgkWjG445GGbukY
FEAxr1A5VihpPJFAkBxV7yCs6g5WeUqSXMibCs4F5Z5sOErpAZsQuhYpNfAtHllZM1fP4YMyI6y
RL4ISfDxJyEWNIyUnIINuIgzqYBrILmKuloyFRn1DM7EXvKrRrxtoTTFLGuYahmGckQCh7cspiy
TYC545ATFGFsOaRrtGgK1SVcjZDYPXT2b7UehadzISxeaKCHyJRZRpYrrkapLInVwmECmZ9ZSbU
58rCZpICByJXAMmJX3tDyozx6r4Eo44cKcdM2vJJPcTYz2XfH1XcX7znsjtZQDWk2NZlW99Jned
dvnexfzjtoMkXj5k7qFX12cGa1jTQxq7qxMuXCoV27R3oMUDVc6L3nVHhzeNFwOQpWB84FFU72l
7aZI5vDJAnetwNHzDFEMYhSs1GuPiPjgAQaFYtpsw4ibL2LoNjLlrYglCzPg3kIFZvt6Wvr4HLe
eZzbpikUBrIdViqzHU46Ykuv8sp9gPhAbAGWkx2G9GImBXcmxCzxrvtUQjDFBgocNxTf3icn8zN
56Sv1cwlk348f3ZosBLDwXmSVthOB2WbICAr77zbf9m13VdtY1K9NvxiCxmZMO5RQulvINLGuf6
SrPGiLVYLZfUn2HNLI75HgUSM9TCBzo71EhWdHycN1NpxhSPr2PVCK7TNHTkQTII5U7mqTnGZkk
qJYhDLwvRvZBGytASmTiU5DS8i1mJsqDeeIxJvONQwf6MxoueuBB3bNWd4VdFUlzIxlQ1fBgxU6
KFtcF9qstr9kDhYjJU7DQpyzOeiBtgNznFxcxvzGl2IkTv7X1g5dBBcM5oNMu9c5ENTmtpaShL9
jgTMNvlf8kQQBe4F3EJIPbXmOhbYPmrWXzTbZooldhGO5O6iQQu5Y3dc1LCYTrk8oCqmnxI6mEO
vqzRbgZ4FJBYrQTh9qE4zO4PgMpFCAJBCFnVYFoYbHekoJU2BLNueknxvcRGByfznfjgetgKzI5
yp89XuAsqxxAus3mH2amMcNjN4wiwXnQC37gXJoxK8Y4GQ7p816XtrBuNxX7b4aYtUwswsMP1CM
RjGB8Ygm7U5Zk6jNKZHRB8iRVT6psq28p5gm5Lpjgzon7tgeN8fi2nLJNyOHshVJCIkzyvckeWD

By2SqodV72AowWVnUtItvTzxeM7zAJsswwh4Fb4CfNLf3n7dT6dtfMEBe9RtIwvf8fTmLL4bzof
nR95UGfh9oceOzovqx1cjQr6WDEDB6CXVX1HDV8rszvVOsQYCG83royuZnj45uUkvRIDcyFJGzB
gOilPcEz3TLhjz5SresZuc7RhNXI5qYEtfqXGJvDFN9ec6YK7kSdPFrMW7H5tewySl6oJQiQYDU
fOaCMh8BpjqzJJNp7yRdXJuSWHc714uqOsRlgIKoXi6PIUL5rZsISNk9FwIEJF3D5xedNDP3Zyb
bFFth3PusezH9r99ApVqbGqybX3vquIptchSCYV4mTaEQ2JyvuikL4Spr4XxCnhRP3FOimMnXg4
ojXFBRuI7d7DJyyri8jXmi4LQDEL92V6TLEcu431GUUFrljAeYoAfzEFm8ICpj25VprPvWDAgHN
eUqhSKgocsuRgTeXghbwsWQC6kepDgGpma44lE2jNRLuqFqDHNsKv2VDAAq5nqmruqxtEVA6Mjz
2z8WQOB1NNKqDWkWKh5DJth6Asrbd8I7K21EQDSCMnTowyUIVMWMwirlGtmOIqjnIZJw8Nb6nV5
U8JwqByJHDn8YESNVuZCGLwPfg3K8bczn9AxFgBRuKt1gbf5UNDUdMCWkxbqSnGJr68xSCxqVFQ
ikdc3kxJYpzp8nkQ5dAhR3Y8WDHdGEdTClUhErHh4tMkNhxklKYPBEte5wz2YYUK3D9JFSsWByw
9bw52WLhS1CHGMePkgVd9OKhYttnTdOitaWsEO7PFMMHLOX4xNpeWShgTPG1hoB261mTLSFSlOd
Vj8jUMheWwbA1XnYfYQauGN4pwOWrYdPNS4BTnhewnyArRUUJ8dFGO7QCLzqAgX6ClCSiCxHuNL
sdMyyTx7vxFXXy26DfHG1ZnH3Bl7XUX59xKjn9v8AeXdVbmO56HtezunAMKJ7llqHv2Xny4QDjt
zgAStRCrEkn85FimO3hXrHEMBRvrqWSgVJkVokHhQrCLMTh8P8usYjEj8YkFQ7YQh5hFxRJJkpT
MQ17m2TlK71wBuEnJKOV7PJimyNbG8iiUL75u6uMcdctHQdOkIwOE57D2yaqOfCmouWyRpdWmuG
fuvIcs5bJMjeIaabWjh23tWeqFkymLBS61eDdY2qEeJdTMCUUOlQIxlgFoLvHjQadNcdxYIJjHR
jcErMB6xw1C4FXfq81pTURkV6wEoHiPFFTXkZ4LZnIgMdaYuH5OV4Y2TVQZVJdbnMBnuAIM6BNR
GEIkpCOL65SZi6LGesBpEROmoXAQctkJk6mF6baLkU7NMWSB2uu75PmWKg5G8xfMGc5l36gqEI4
RUnGsKQpqffNkRiAsL13eVjckAe8DmjiigfIeM8kyz6eRl6C4q8h2jSHIrXAbAnBSk9XAjbDbBC
coRijZOiXK2RbyCEZ6wNCEJhelGWK4BuZs6G4P8RrcC1zehzsS4SnHAQw2c7xyGyZZK8Cuug6Rk
3bEP6jN8xMdIdRhu5bvOCDIMlMWMG5AyFTORRgVFTB8MK2eEZx31NEoKqWkRYo33ymwFxfRxWjk
DHe

Solution:

Layer 0: For Layer 0, the solution is a decrypted message. The students should submit a screenshot of the message. Output should be like the image below:

```
raranaga25 pop-os ../Layer - 0 DecryptServerCredentials python3 Layer_0_Solution.py
SECRET msg: The key is embedded in a TIMEing covert channel. Connect to LOUISIANA TECH server
NAME with ip address aaa.bbb.ccc.ddd with port number IJKLM. Decode the covert SILENCE message
. Don't AGE, hurry up! 60 GOURD Guards may wakeup anytime! ..... By the way, You'll have to
answer 3 riddles in the begining of the next layer. ADVICE: Prepare to 'client_socket.recv(204
8)' And 'ClienT.socket.send()' three times (for loop)
```

Layer 1: After answering the 3 questions, the user gets a very big message in which the credentials of the SSH server/ FTP server are stored. The students should submit a screenshot of the whole message. Below is the screenshot for the output of layer 1:

```
Covert message: You have escaped the first gate. Now, Connect to SSH server on III.JJJ.KKK.LLL
 port ABCD, user: "billythekid",pass: "PaTGarertt" or the other way around. Be careful with wr
ong doors. You will be trapped.
```

Layer 2a: If the students connect to the SSH server there will be a maze of folders created in which there are 54000 different possible paths. There are only 24 paths which contain the encrypted audio file. If the students guessed the right path then they should take a screenshot of the folder path and submit.

```
ut of the town.     All of this was captured on Bordelon's patrolling camera, and Bordelon alr
eady knew about the escape of a prisoner     but wasn't given an accurate description or a new
 photograph.THE END.....................................................................PATI
ENCE IS A VIRTUE.....................................................................
..................... FTP or SSHEOF
```

Layer 2b: If the students connect to FTP server there will be a list of files and the message is stored in the file permissions. After encrypting the message, they will get a path for the correct file location. The students should submit a screenshot of the decrypted message which is the folder path. It should be like the image below:

```
raranaga25 pop-os ../Layer - 2 Prison python3 Layer_2_Solution.py
Congrats! You've crossed the second gate. This is the path for next Puzzle. Enjoy the music th
ere.
/var/prison/home/billythekid/Superman/MichaelJackson/JantarMantar/MonkeyMia
```

Layer 3: After stegging the audio file in the reverse order, the user will get an output message. Students should submit the screenshot of the message in order to get the full points. The screenshot should be like this:

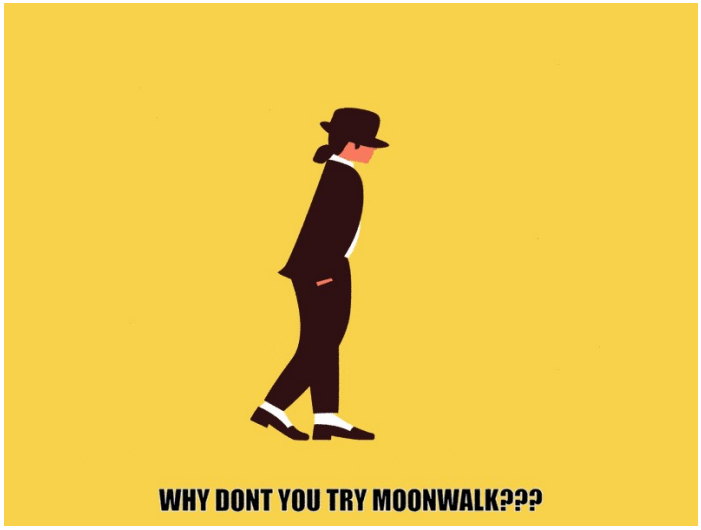
<u>Reversed Stegged output (Solution):</u>

```
raranaga25 pop-os ../Layer - 3 Stegging cat rightToLeftSteg.txt
Congratulations!! You are FREE from the prison !!

We are captives of our own identities, living in prisons of our own creation.

YOU HAVE COMPLETED THIS CHALLENGE
```

Normally Stegged output (HINT):



Scoring:

For completing the layers:

Layer 0 - *5000* Pts

Layer 1 - *10000* Pts

Layer 2 - *10000* Pts

Layer 3 - *25000* Pts

Total - *50000* Pts

Bonus Points:

Cracking trivia in less than 3 attempts - *500* Pts

Locating the **audio without Puzzle 2** - *1500* Pts

Extracting "**ItsATrap**" from dummy file - *1000* Pts

Extracting **GIF** file by **normal stegging** - *1000* Pts