|  |  |  |
| --- | --- | --- |
| Date | Hours |  |
| 19/12/22 | 4 | I started my project by learning a bit of socket programming on YouTube videos and was able to create an elementary program that worked. |
| 20/12/22 | 5 | I started to think about the micro teach and the subject to do and decided to go with a reverse shell. I found it fascinating how it completely bypasses modern-day firewalls due to being an outgoing connection.  Although I found very little information on to create one, I found some videos, so I started learning about it. |
| 21/12/22 | 5 | Carried on learning.  I now know the basics about a simple shell and how it works |
| 22/12/22 | 4 | I managed to finish the client and server reverse shell, but this would only work on the local network, so it wouldn't be much use, although there is a great learning curve.  I decided to look for more on the subject, and after many websites saying how "dangerous" it was, I found a complete course on it. |
| 23/12/22 | 5 | Python basics refresher |
| 24/12/22 | 1 | Python basics refresher Merry Christmas |
| 02/01/22 | 3 | Python refresher |
| 03/01/22 | 4 | Finished python refresher |
| 04/01/22 | 4 | Started a course on app development in python  Also started to learn more about socket programming. |
| 05/01/22 | 2 | Created a server that echos the client input |
| 06/01/22 | 4 | Created basic chat server  Scrapped my idea to make a dating app as it would take to much time and not focus on security aspects as I want. |
| 07/01/22 | 5 | Created a multi-thread chat server where I can open various clients that connect to an IP / port |
| 08/01/22 | 5 | I started working on the app to create GUI where you can see the chat in a window  Run into many issues, like how to figure out to make a button work or do a command  Worked on the micro teach |
| 09/01/22 | 4 | *Basic GUI completed*  *Worked on the micro teach* |
| 10/01/22 | 5 | *Advanced GUI started, and it is slightly more manageable now that I know what I am doing.*  *Worked on the micro teach* |
| 11/01/22 | 6 | Advanced GUI is finished, but some functions are not working, but the interface is all present and reasonably present, and warnings are showing with the lambda command, but unable to fix it or find any way to do it.  Showed work to the lecturer and found the additional problem as the kick and ban not working |
| 16/01/22 | 2 | Restarted the project, after the conversation with the lecturer, realised that my project did not meet the requirements so returned to basic code to work on RSA encryption. |
| 17/01/22 | 2 | RSA encryption working on a single file, started implementing on sending it over the server, but unable to produce any results |
| 18/01/23 | 5 | The KICK and BAN buttons fixed  I missed something self-evident, but I couldn't see it for ages.  Text  Description automatically generated  New theory on the RSA encryption, the volume might be to big so returning to my advanced GUI way of encryption, so ill be trying to: Capture the input > change to ascii > encrypt with key > store in a JSON file > send it over  Hopefully reverting the process wont cause problems |
| 19/01/23 | 8 | Attemping to not implement JSON for testing    Update: DOESN'T WORK  Although stuck on how to receive messages    As I don't know to put in the byte size, what size should I set ? as encoded messages could get big  It looks like I have just been doing it all wrong and don't understand the concept  -----------------------------------------------------------------------------------------------------------------------------------  I can't encrypt and turn it to JSON because JSON only works with dictionaries or lists; it suited me perfectly for what I wanted to do with the flag states, although I do not see a way to make it work with RSA encryption.  The thought of having spent so long creating an app that works perfectly to scrap it is depressing.  --------------------------------------------------------------------------------------------------------------------------------------  Grabbed some old code where is a simple single thread chat system and implemented RSA encryption, I pretty much completely over thinking it , as I was encodying it and trying to send it but it just wasn't working, with a lot of debugging using print and print type I have managed to figure out the issue, so made it work, but I was getting an input then store it then encode it then turn it to a string then encode it in uft-8 to send it over the server, needed to decress the number of steps.  So I reduced the number of steps but I broke something and wasn't working, so I decided to remove the utf8 as why do I even need to encoded something that Is encrypted and in bits ?  So its working! |
| 20/01/22 | 6 | After getting the single thread working yesterday, I decided to go for multi-thread, thinking the process would be the same; luckily, it was well, so I thought; the encoder did not agree with the way I produced names followed by the message, creating a lot of issues and not allowing me to decode as I think its because decrypter is trying to decipher two different things at the same time, so after deleting the name it started working fine confirming my suspicions, that brings me to my main program, where my entire program sends information back and forwards in a dictionary in a JSON due to finding a website that said Json encoding was safe, but I don't think it's good enough for what the lecturer waiting to confirm with lecturer soon; meanwhile I need to try to find a solution, I am thinking about isolating the input message encrypt and then add to the dict and send it over. But that's easier said than done.  In one of my research, I found there is something to encrypt the actual JSON, and its AES, so it falls under advanced security, so there's another possibility, but that would negate all the work I have been doing and would be another thing for me to learn; so for now.  Decided to try to learn how to encrypt JSON but yet again ran into the same issue that has been plaguing me since the beginning, I can not install the library Crypto, so I am stuck.  Reverting back to the original idea, encoding the message in a dict seems to work, but while encoding the json creates an error due to the encrypted message being in bites, |
| 21/01/2023 | 4  2 | Still havent found a way around it, due the way encryption work any attempts of changing the format change the code as well, so my current method of encoding is not working, for my main program, as I need to add all the information in to a dict as a string.  Last chance to save my project is to somehow try to encrypt JSON  Or  Try to send the message separate from the JSON but that would involve a lot of changes, pretty much just create a new program  Cant get anything to work…  I am too tired, given up…  Created a basic chat program that is all encrypted with timestamps and nicknames, although found a bug, when the nickname is bigger than 1 letter it doesn't decrypts |
| 23/01/23 | 2  3 | After starting an entirely new project, I went through the requirements list.  I have implemented a function that detects when the word QUIT is used and closes the connection, and the server detects when the user left and broadcasts to all the users that person left. N2  Using a multi-threaded approach so N1  Basic error handling messages N3  RSA encryption S1  After the chat with the lecturer, I realised I could actually salvage the project that I had spent so long on.  I can use Ceaser cypher as the output is in the form of a string, so I can carry on using JSON to send information back and forward.  Although if I am unable to implement Ceaser Cypher, I can revert to my project as I have already done enough for 40%  Funny note my cypher doesn't allow capital letters; I spent an hour trying to figure out why, hahaha  Only understood why because my name I was writing Bruno, and it was coming out as Vruno  Fix: force lower() on inputs  Unable to create an async chat after my first message chat starts spamming.  Looking for a solution  I tried removing the encoder, and it goes straight to spam, so I guess its something to do with the encoder and decoder  Can not figure out what is causing the problem.  Will attempt to implement on my main program as I grabbing the input and encrypt straight away without passing trough anything  And as its part of a message pack its easier to isolate without having to be messing around encoding and decoding commands etc  Encryption completed display correctly on server side but not on client will carry on tomorrow but its progress!!!!!!!!!!!!! |
| 25/01/23 | 4  2  2  1 | Several issues fixed that were introduced by the encryption  Broadcast messages display correctly  Messages same  Pm same    But the problem about the capital letters still remain  Appending to change the script to count for this problem or force lower to avoid problems  Forced lower to avoid problems if theres time ill come back to it and change  Add an id “tag” to the program  Now users have an id admin id is 0  Trying to implement the Diffie Hellman but clueless how to implement it on my program… again without changing everything.  Trying to implement a id swap to try to create a Diffie Hellman broke something and now the program does not work |