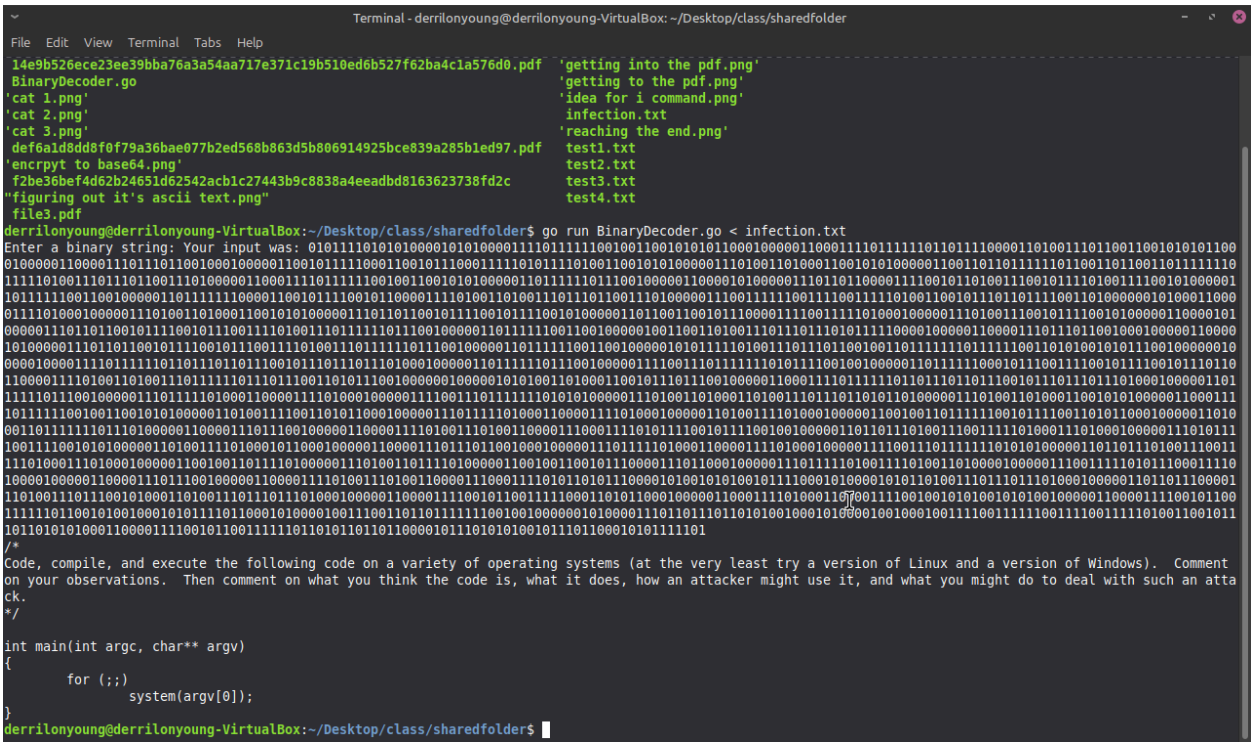
Chandler Dees, Caleb Davis, Prashant Neupane, Derrilon Young, Nikolaus Krause (Mothman)

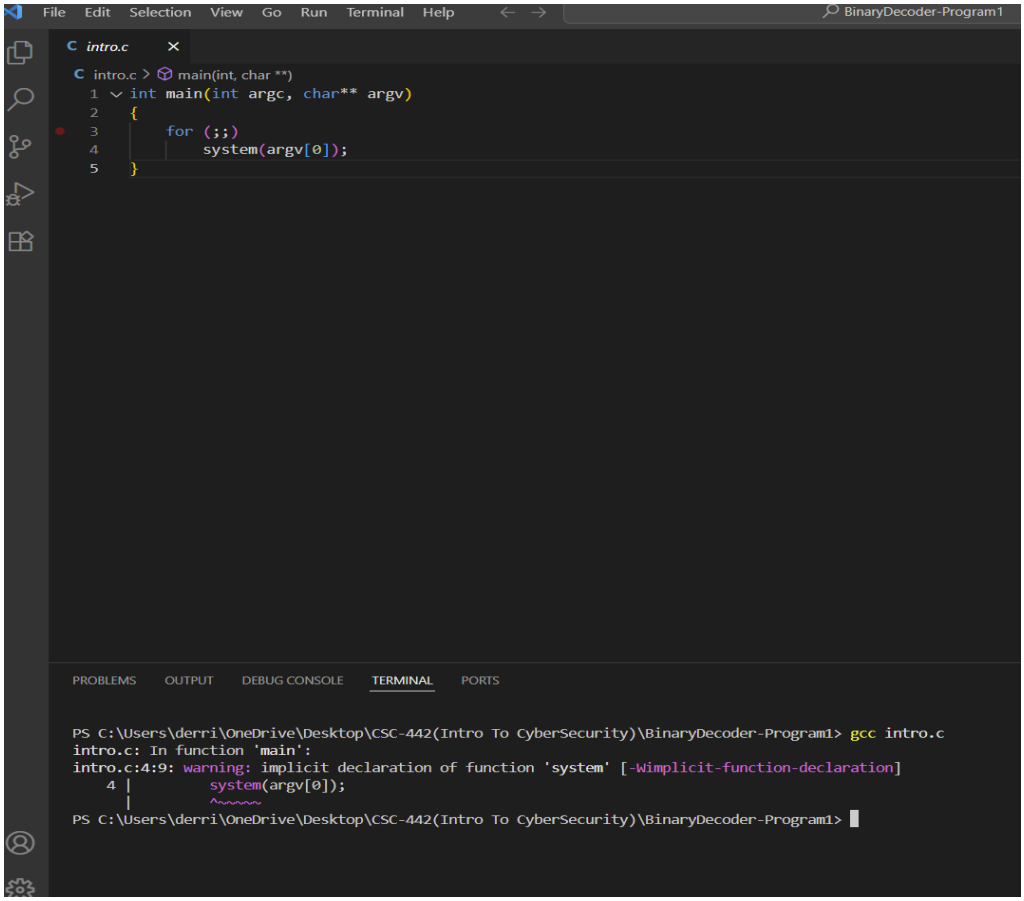
Per the instructions in the binary pdf on Canvas:

After running all of the test cases and getting the intended results back for each one, the infection.txt file listed alongside the test files was also run through the binary decoder file. The result was as follows:



As shown in the screenshot above, the binary string within the infection.txt file was compiled and run and the bottom portion of code was produced from decoding the string.

The code below was determined to be C, and the instructions were followed pertaining to the given code. After running the code, this result (listed on the next page as a screenshot).



After showing the code and the result to the rest of the team, we agreed that the code seems to be creating and running an infinite loop that executes what is input into the command line with system permissions. We also agreed that since the code only checks the first argument that something like “sudo” would be dangerous because it would grant the user access to everything on the computer (with the assumption that they have the password). There was also a discussion regarding how the code could be used for a “denial of service” attack, meaning that someone could be kept from accessing the server because it is being kept busy.

We believe that we could deal with an attack like that by checking for and limiting certain keywords from being used. If this is violated, the program would terminate or a warning would be printed to the screen.