# Osiris Challenge 2

**Decoded PDF Message:**


Congratulations on getting to the end of this challenge. Hope that was fun.

Don't forget to document your process and upload all relevant documents/files to Moodle.

**Time decoded:** 11:32AM

**Description:** Upon Reverse engineering the provided 1.exe file we discovered an FTP server with default logins. We then used the fetch.py 7-bit program to read the permissions which led us to an alternate log in within the same FTP server. After exploring the new FTP server login we came upon a Hint.class Java file which we concluded was a distraction. Thus we decided to delve even further into the FTP server in which we found a second executable file called 2.exe. Finally after reverse engineering this file we found the hashed password for the PDF that we dehashedusing https://hashes.com/en/decrypt/hash to get the final password, "letmein2". Then we put that password into the prompt that pops up when trying to access Final.pdf, rewarding us with the decoded image message.

**Team Contributions:**

Ethan Hebert: Logged onto FTP server and found the Hint.class file. Tried reverse engineering this but got errors with the version of the Class file. We think this Hint.class file was a distraction from finding 2.exe.

Noah Jones: Discovered 1st FTP server, Hint.class,hashed pdf password 2.exe file, reverse engineered 1.exe and 2.exe file.

Keaton Love: Analyzed 1.exe, Hint.class. Attempted to dehash password. Provided feedback to support problem solving.

Jace Peloquin: Formatted google doc, moral support, team mascot, helped brainstorm ideas

Amiyah Frierson: logged into FTP server with credentials, hash decryption attempt

Madeline Ballew: logged into FTP server, went into hidden directories all the way down, decoded final hash to log into pdf, and logged into pdf

Jay Reich: logged into the FTP server as anonymous and used the FTP decryption program with the 7 bit method to find the username and password. Nyeh heh heh!