

Challenge #1: Getting Permissions

Objective

The goal of this challenge is to discover covert messages that are being “sent” through an FTP server: **You Shall Not Pass FTP Server** (FTP server specifics will be provided at the beginning of the challenge). The FTP server sets a covert message by craftily creating files/folders and modifying their permissions appropriately. It is designed to wipe all files in the appropriate directory on the FTP server every 60 seconds. It then creates a new message (in binary) and encodes it by creating as many files as needed, modifying their permissions appropriately. So yes, the message changes every minute!

The covertly transmitted message is restricted to characters in the basic ASCII character set (ASCII values 0 through 127). Whether the covert message is encoded using all 10 permission “bits” of the files/folders on the FTP server (or just in files that have the right-most 7 bits set) must be determined. Moreover, where these files are located on the FTP server must also be determined. So...explore...tinker!

Your decoded message must match the current message being transmitted since it is changed every minute. When you think that you have successfully completed the challenge, post your decoded message in your team Discord text channel and @ prof.

As a challenge deliverable, please submit a ZIP file, containing the following items, on Moodle:

- (1) A document that provides a **thorough** summary of your team's completion of the challenge. The document must include: **(a)** the decoded message; **(b)** the time at which you obtained and decoded the message; **(c)** description of the steps you have taken to obtain the message; and **(d)** description of **each** team member contributions. Please note that **each** team member should contribute their own paragraph to this document that describes their role in the challenge.
- (2) Any modified Python code (e.g., major modifications to FTP, Vigenere, Binary programs); and
- (3) Any other scripts or programs that you created to assist you (if applicable).

You will be graded on how well you:

- (1) Determine the FTP login information (10%);
- (2) Determine the FTP login credentials (20%);
- (3) Obtain and decode the covert message (matching the current time) (45%);
- (4) Document your process (20%); and
- (5) Submit the required ZIP file (5%).

Good luck!