Exercise

Introduction

The attached code implements the communication protocol between malware and its C2 server.
Like every malware, this protocol is exposed to variety of threats in the wild, such as: IDS/IPS products, threat haunters, incident response teams, etc.

Your Mission
As a security researcher you are asked to perform the following tasks -

1. Identify and list, as much as you can, implementation gaps in the communication protocol which are may exposed the malware traffic and allow its investigation.
2. Offer and implement an updated and more secret protocol that addresses the gaps you mentioned in the previous section (choose your preferred language: Python, Go, C#, etc.).

As part of the examination all components must be considered: client, server, home page.

Notes:

The solution will be sent as a compressed zip file with the following content –

1. A textual file which describes and explains the security gaps you already identified.
2. A directory with the code files of your implementation as well as explanation of the solution.