Project Tracking

Offensive Computer Network Operations (CNO):

- **Quite-Knight**: Developing a C based implant compiled for Windows systems which can accept and parse offensive cyber commands. Along with the implant we will also be developing a Python based server which can be run from any platform to serve commands to the C based implant. The servers implementation can be changed in the future to be based on a web interface for example. The goal of this project is to familiarize myself with offensive exploits for Windows platforms as well as gaining experience with the WinSoc API. Quite-Knight will implement the exploit vectors laid out by Snowy-Ghost.
    - **Snowy-Ghost**: Finding and exploiting a vulnerability in a default Windows application or service. To complete this task the vulnerability needs to be documented with a clear exploitation vector. This will include analysis with Ghidra if necessary. The exploit(s) found within Snowy-Ghost will be used in Quite-Knight. To complete this task at least three vulnerabilities will need to be analyzed and documented.