I was able to successfully established communication between my C2 server and client, and enabled file uploads to the server:

A black background with white text

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

However, I have been encountereing challenges while attempting to integrate pfSense with an external network and install Snort. Despite configuring the settings in the lab environment as outlined in the screenshots below, including assigning it a separate interface and verifying connectivity to both LAN and WAN, I have been unable to access any sort of external networks to complete the Snort installation thus far.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

At this point, I have still been unable to resolve this issue despite multiple attempts. I understand and apologize that my submission is incomplete, and I am actively working on resolving the problem. I was not expecting this much of a struggle as I have worked with snort and network communications before. However given the assignment is deadline is soon, I want to submit this to ensure that I have something turned in. I will hopefully reupload before the deadline with a completed assignment.

Update:

I am able to run suricata separately on my client vm:



A screenshot of a computer

Description automatically generated

As shown below, it is successfully sniffing the contents of the data sent from the client to the server:  
A computer screen with numbers and letters

Description automatically generated

This also works when the file contains a SSN:

A computer screen shot of a computer code

Description automatically generated

Since I do not have the GUI inside pfsense, I am working to modify the rules manually inside /etc/suricata/suricata.yaml.