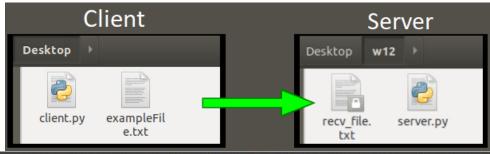
I was able to successfully established communication between my C2 server and client, and enabled file uploads to the server:

```
dsu@dsu-virtual-machine:~/Desktop$ sudo python3 client.py
[sudo] password for dsu:
[*] Received File Path: b'/home/dsu/Desktop/exampleFile.txt'
[*] File Contents sent to Server
```

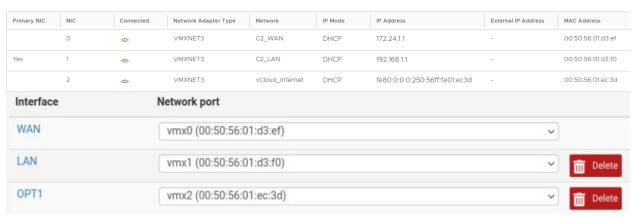
```
dsu@dsu-virtual-machine:~/Desktop/w12$ sudo python3 server.py
[sudo] password for dsu:
[*] TCP server listening on 192.168.1.104:80
[*] Accepted connection from 172.24.1.2:37968
[*] File path sent to client: /home/dsu/Desktop/exampleFile.txt
[*] File Received from client
[*] File Saved
[*] Received Contents:
Super secret contents
```

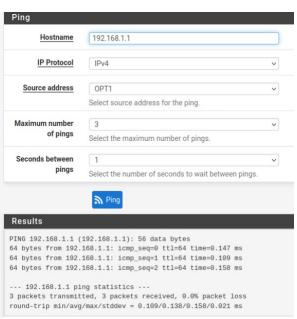


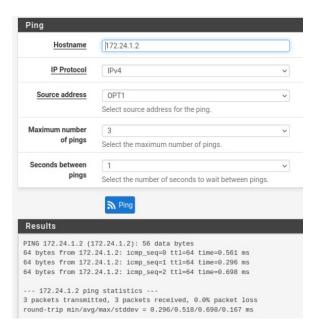
Packet Capture Output: /tmp/packetcapture-vmx0-20240419062346.pcap

```
11:23:54.949251 IP 172.24.1.2.53334 > 192.168.1.104.80: tcp 0
11:23:54.950170 IP 192.168.1.104.80 > 172.24.1.2.53334: tcp 0
11:23:54.950515 IP 172.24.1.2.53334 > 192.168.1.104.80: tcp 0
11:23:54.951337 IP 192.168.1.104.80 > 172.24.1.2.53334: tcp 33
11:23:54.951524 IP 172.24.1.2.53334 > 192.168.1.104.80: tcp 0
11:23:54.952018 IP 172.24.1.2.53334 > 192.168.1.104.80: tcp 0
11:23:54.952242 IP 172.24.1.2.53334 > 192.168.1.104.80: tcp 0
11:23:54.952292 IP 192.168.1.104.80 > 172.24.1.2.53334: tcp 0
11:23:54.953064 IP 192.168.1.104.80 > 172.24.1.2.53334: tcp 0
11:23:54.953064 IP 192.168.1.104.80 > 172.24.1.2.53334: tcp 0
```

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.







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:

```
dsu@dsu-virtual-machine:/etc/suricata$ sudo systemctl start suricata
dsu@dsu-virtual-machine:/etc/suricata$ sudo systemctl stop suricata
```

```
dsu@dsu-virtual-machine:/var/log/suricata$ cat stats.log
Date: 4/19/2024 -- 07:47:41 (uptime: 0d, 00h 00m 08s)
                                              | TM Name
                                                                          | Value
capture.kernel packets
                                              | Total
                                                                          | 56
capture.afpacket.polls
                                               Total
                                                                           95
capture.afpacket.poll_timeout
                                                                           58
                                               Total
capture.afpacket.poll_data
                                                                           37
                                               Total
decoder.pkts
                                                Total
                                                                           56
decoder.bytes
                                                Total
                                                                           4838
decoder.ipv4
                                                                           52
                                                Total
decoder.ipv6
                                                Total
                                                                           4
decoder.ethernet
                                                                           56
                                               Total
decoder.tcp
                                                                           24
                                                Total
tcp.syn
                                               Total
```

As shown below, it is successfully sniffing the contents of the data sent from the client to the server:

```
      dsu@dsu-virtual-machine:/var/log/suricata$ cat tcp-data.log

      172.24.1.2_57812-192.168.1.104_80-tc:
      0000
      2F 68 6F 6D 65 2F 64 73 75 2F 44 65 73 6B 74 6F /home/ds u/Deskto
      0010 70 2F 65 78 61 6D 70 6C 65 46 69 6C 65 2E 74 78 p/exampl eFile.tx
      0020 74
      t

      172.24.1.2_57812-192.168.1.104_80-ts:
      0000 53 75 70 65 72 20 53 65 63 72 65 74 20 43 6F 6E Super Se cret Con
      Super Se cret Con

      0010 74 65 6E 74 73 0A
      tents.
```

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