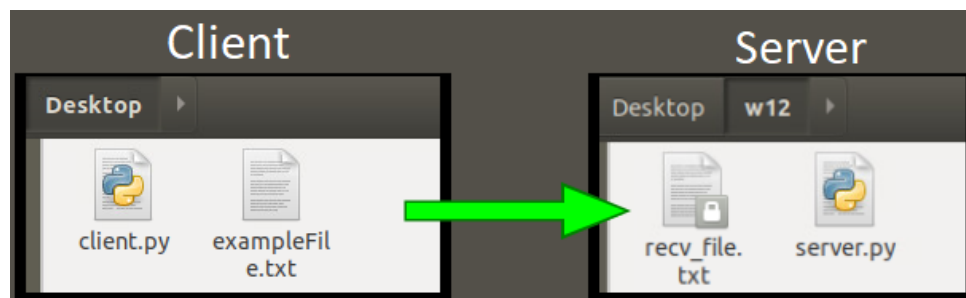


I was able to successfully establish communication between my C2 server and client, and enabled file uploads to the server:

```
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 22
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
11:23:54.953272 IP 172.24.1.2.53334 > 192.168.1.104.80: tcp 0
```

However, I have been encountering 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.

Primary NIC	NIC	Connected	Network Adapter Type	Network	IP Mode	IP Address	External IP Address	MAC Address
	0		VMXNET3	C2_WAN	DHCP	172.24.1.1	-	00:50:56:01:d3:ef
Yes	1		VMXNET3	C2_LAN	DHCP	192.168.1.1	-	00:50:56:01:d3:f0
	2		VMXNET3	vCloud_Internet	DHCP	fe80:0:0:0:250:56ff:fe01:ec3d	-	00:50:56:01:ec:3d

Interface	Network port
WAN	<div>vmx0 (00:50:56:01:d3:ef) </div>
LAN	<div>vmx1 (00:50:56:01:d3:f0) </div>  Delete
OPT1	<div>vmx2 (00:50:56:01:ec:3d) </div>  Delete

Ping

Hostname

192.168.1.1

IP Protocol

IPv4

Source address

OPT1

Select source address for the ping.

Maximum number of pings


3

Select the maximum number of pings.

Seconds between pings

1

Select the number of seconds to wait between pings.

 Ping

Results

PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=0.147 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.109 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.158 ms

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.109/0.138/0.158/0.021 ms

Ping

Hostname

172.24.1.2

IP Protocol

IPv4

Source address

OPT1

Select source address for the ping.

Maximum number of pings


3

Select the maximum number of pings.

Seconds between pings

1

Select the number of seconds to wait between pings.

 Ping

Results

PING 172.24.1.2 (172.24.1.2): 56 data bytes
64 bytes from 172.24.1.2: icmp_seq=0 ttl=64 time=0.561 ms
64 bytes from 172.24.1.2: icmp_seq=1 ttl=64 time=0.296 ms
64 bytes from 172.24.1.2: icmp_seq=2 ttl=64 time=0.698 ms

--- 172.24.1.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.296/0.518/0.698/0.167 ms

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)
-----
Counter | TM Name | Value
-----
capture.kernel_packets | Total | 56
capture.afpacket.polls | Total | 95
capture.afpacket.poll_timeout | Total | 58
capture.afpacket.poll_data | Total | 37
decoder.pkts | Total | 56
decoder.bytes | Total | 4838
decoder.ipv4 | Total | 52
decoder.ipv6 | Total | 4
decoder.ethernet | Total | 56
decoder.tcp | Total | 24
tcp.syn | Total | 24
```

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

This also works when the file contains a SSN:

```

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
0010  74 65 6E 74 73 0A  tents.
172.24.1.2_46688-192.168.1.104_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_46688-192.168.1.104_80-ts:
0000  38 36 37 2D 35 33 2D 30 39 30 30 0A 867-53-0 900.
dsu@dsu-virtual-machine:/var/log/suricata$

```

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