

8505 Assignment 1

Peyman Tehrani Parsa A00922386

September 24, 2018

| | |
|--------------------|----------|
| Code review | 3 |
| Design | 4 |
| Requirements | 4 |
| Usage | 4 |
| State diagram | 5 |
| Testing | 6 |

Code analysis

Craig Rowlands covert channel weaknesses were that

1. his code only sends one byte at a time
2. The send interval can't be controlled

I would improve on it by sending the data in three fields at the same time to increase bandwidth. TTL, source port and, sequence number which can transport two characters if used correctly.

Design

Requirements

Scapy is needed for the program to run correctly please download and install from

- the Github repository (latest development version):
<https://github.com/secdev/scapy/archive/master.zip>
- the Github releases page
- dnf install python3-pip
 - pip: sudo -H pip3 install -U scapy

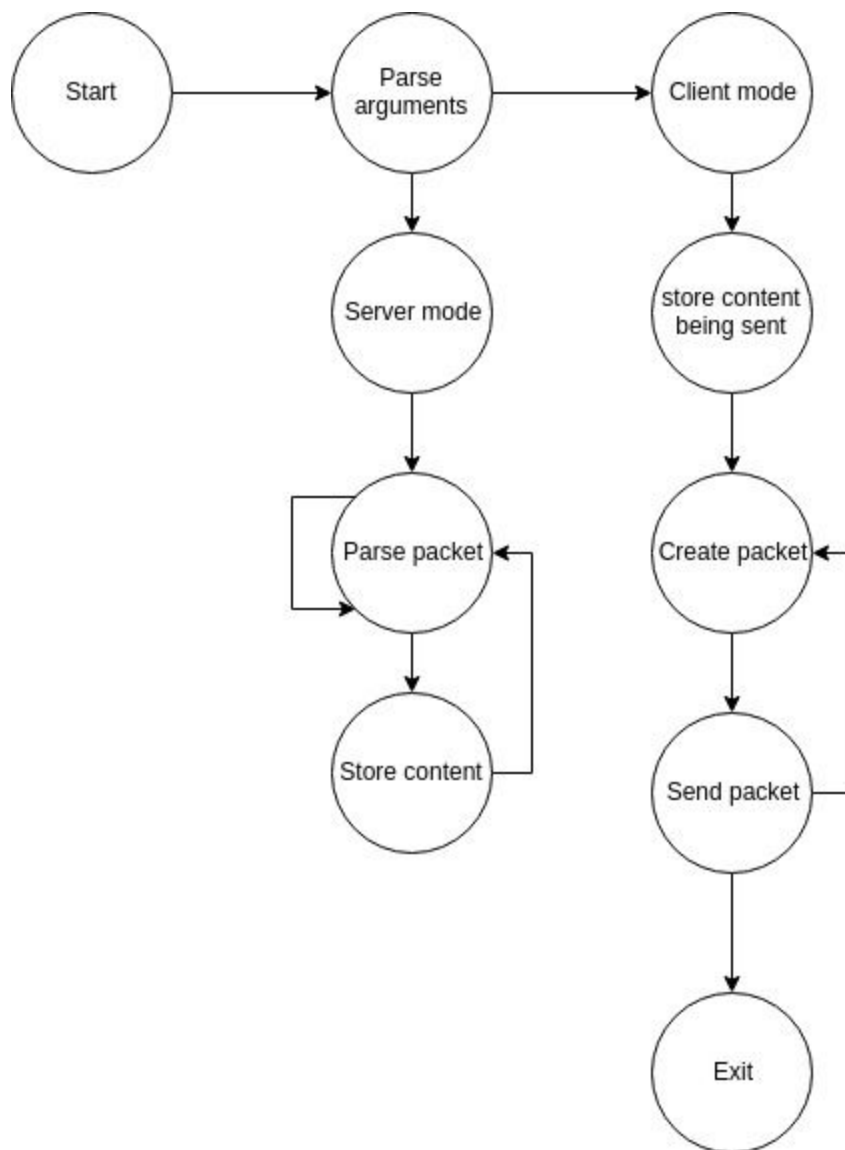
Usage

```
usage: Covert Channel [-h] [-s SRC_IP] [-sport [SRC_PORT]] [-d DES_IP]
                        [-dport [DES_PORT]] [-f FILE] [-msg MSG] [-t TRANSPORT]
                        [-mode MODE]
```

| | |
|-------------------|---------------------------------------|
| -h, --help | show this help message and exit |
| -s SRC_IP | IP of computer being bounced off of |
| -sport [SRC_PORT] | Port of computer being bounced off of |
| -d DES_IP | IP of server |
| -dport [DES_PORT] | Port of server |

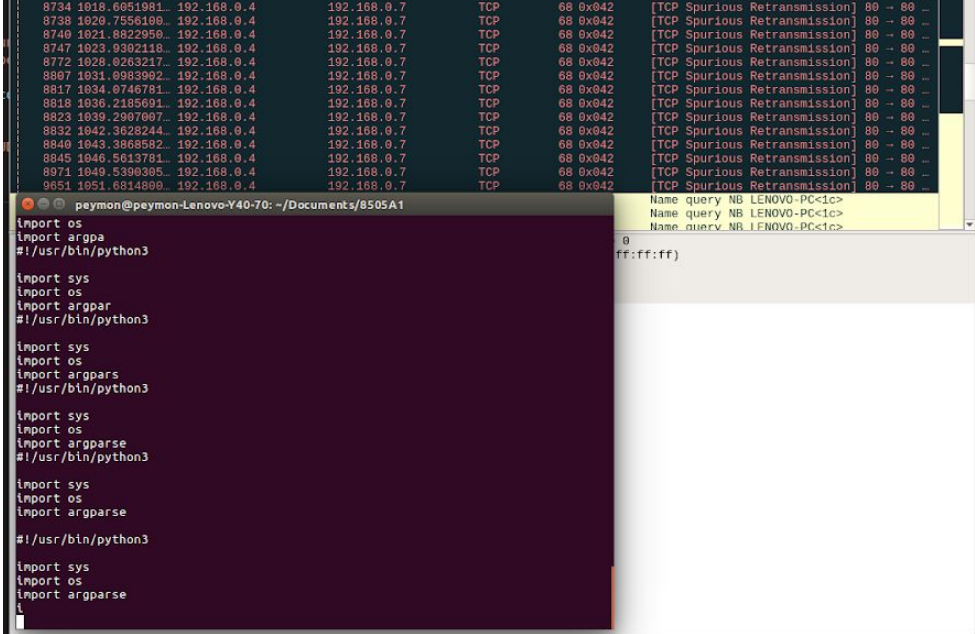
-f FILE, -file FILE File being sent
-msg MSG Text being sent
-t TRANSPORT, -transport TRANSPORT
 TCP or UDP
-mode MODE server or client

State diagram



Testing

| | |
|-------------|--|
| Test# | 1 |
| Description | Sending packets over covert channels |
| Steps | Note: must have scapy ./sneaky.py -s 192.168.0.4 -sport 80 -d 192.168.0.7 -dport 80 -f ./sneaky.py -t TCP -mode client |
| Expected | Packets sent without error and correct fields filled in |
| Result | <pre>root@CM-Desktop:~/Documents/BTech/8505A1# ./sneaky.py -s 192.168.0.4 -sport 80 -d 192.168.0.7 -dport 80 -f ./sneaky.py -t TCP -mode client reading file b'E\x00\x00(\x00\x01\x00\x00#\x06\x16t\xc0\xa8\x00\x04\xc0\xa8\x00\x07\x00P\x00P\x00\x00\x00\x00\x00\x00\x00PB \x00\r\xa7\x00\x00' . Sent 1 packets. b'E\x00\x00(\x00\x01\x00\x00!\x06\x16t\xc0\xa8\x00\x04\xc0\xa8\x00\x07\x00P\x00P\x00\x00\x00\x00\x00\x00\x00PB \x00\r\xa7\x00\x00' . Sent 1 packets. b'E\x00\x00(\x00\x01\x00\x00/\x06\nt\xc0\xa8\x00\x04\xc0\xa8\x00\x07\x00P\x00P\x00\x00\x00\x00\x00\x00\x00PB \x00\r\xa7\x00\x00' . Sent 1 packets. b'E\x00\x00(\x00\x01\x00\x00u\x06\x16t\xc0\xa8\x00\x04\xc0\xa8\x00\x07\x00P\x00P\x00\x00\x00\x00\x00\x00\x00PB \x00\r\xa7\x00\x00'</pre> |
| Success | |

| | |
|-------------|--|
| Test# | 2 |
| Description | Receiving and parsing incoming covert packets |
| Steps | Note: must have both scapy and root access <code>sudo python3 sneaky.py -t TCP -mode server</code> |
| Expected | Incoming messages printed out in the terminal And All transmitted packets received and parsed correctly |
| Result |  The screenshot shows a terminal window with a list of network packets at the top, including source and destination IP addresses, ports, and protocols. Below this, a Python script is being executed, which imports various modules like os, sys, and argparse. The terminal output shows the script running successfully, with no errors. The background of the terminal is a dark purple color. <pre>8734 1018.6051981... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8738 1020.7556108... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8740 1021.8022050... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8747 1023.0302118... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8772 1028.0263217... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8807 1031.0983902... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8817 1034.0746781... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8818 1036.2185691... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8823 1039.2907007... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8832 1042.3602044... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8840 1043.3868582... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8845 1046.5613781... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 8971 1049.5390305... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 - 9651 1051.6814800... 192.168.0.4 192.168.0.7 TCP 68 0x042 [TCP Spurious Retransmission] 80 - 80 -</pre> <pre>peymon@peymon-Lenovo-Y40-70: ~/Documents/8505A1 import os import argpa #!/usr/bin/python3 import sys import os import argpar #!/usr/bin/python3 import sys import os import argpars #!/usr/bin/python3 import sys import os import argparse #!/usr/bin/python3 import sys import os import argparse #!/usr/bin/python3 import sys import os import argparse</pre> |
| Success | |