**Cyber Network Security CEG 4430/6430 Project 1**

**Parsing Network Packet Trace Using Wireshark**

Student: Cameron Windsor Fox

**Objective:**

To use the Wireshark tool to perform packet/traffic analysis of a given traffic trace.

This project must be completed individually.

**Pcap File:**

You can download a file of pcap network traffic trace from URL (https:’’www.dropbox.com/s/84cb2s774b8q602/botTrace?dl=0)

Wireshark:

Please download and install Wireshark (<https://www.wireshark.org>) on your own computer or VCSL virtual machine.

You should learn how to use the “display filter” function in Wireshark to facilitate your analysis.

**Questions:**

1. What is the first TCP packet captured in this trace? Please provide the following information for the packet. (2 Points)
   1. Timestamp: Oct 29, 2017 15:58:45.682083000 Eastern Daylight Time
   2. Source IP address: 192.168.1.132
   3. Destination IP address: 192.168.1.128
   4. Source Port: 1177
   5. Destination Port: 6667
   6. Sequence Number (absolute value): 0
   7. Acknowledge Number (absolute value): 0
   8. SYN Flag: Set
   9. ACK Flag: Not Set
   10. RST Flag: Not Set
   11. Packet Number: 31
2. Does this trace contain any UDP packet? If so, please identify the first UDP packet with the following information: (2 Points)
   1. Timestamp: Oct 29, 2007 15:58.58.569547000 Eastern Daylight Time
   2. Source IP address: 192.168.1.129
   3. Destination IP address: 192.168.1.255
   4. Source Port: 138
   5. Destination Port: 138
   6. Checksum: 0x400c [unverified]
   7. Packet Number: 44
3. Is the IRC protocol (application-level) protocol used in any connection in this trace? If so, please identify following information (11 Points)
   1. IP address of the server (2 Points)

Server IP Address: 192.168.1.128

* 1. IP address(es) of clients that successfully established connections with the server (2 Points)

Client IP address(es) that have connected to the server:

1. 192.168.1.129
2. 192.168.1.130
3. 192.168.1.132
4. 192.168.1.134
   1. You can find the IRC protocol at <https://www.ietf.org/rfc/rfc1459.txt>. Does any IRC client generate a packet that contains the following IRC keywords? Please show evidence in your answer. (7 Points)
      1. PRIVMSG: The PRIVMSG keyword is in this trace. See Packet 154 as a reference.
      2. PING: The PING keyword is found in this trace. See Packet 217 as a reference.
      3. PONG: The PONG keyword is found in this trace. See Packet 221 as a reference.
      4. JOIN: The JOIN keyword is found in this trace. See Packet 90 as a reference.
      5. KICK: The KICK keyword is found in this trace. See Packet 47 as a reference.
      6. MODE: The MODE keyword is found in this trace. See Packet 86 as a reference.
      7. TOPIC: The TOPIC keyword is found in this trace. See Packet 133 as a reference.
5. We consider Host-A initiates a failed TCP session to Host-B if the following two conditions are satisfied: 1. Host-A sends a SYN packet to Host-B (to initiate a new TCP session); 2. Host-B sends no packet to Host-A or any RST packet(s) (for this session). For all IRC clients observe in this trace, does any of them initiate more than 10 failed connections? If so, please show their IP addresses and evidence. (5 Points)

Filter to find IP Addresses to test for connection failure:

(ip.src == 192.168.1.132 and tcp.flags.syn == 1) or (ip.dst == 192.168.1.132)

Filter for Testing IP Addresses to check for Connection Filters:

(ip.src == 192.168.1.132 and tcp.flags.syn == 1 and ip.dst == [IP Address to Test]) or (ip.dst == 192.168.1.132 and ip.src == [IP Address to Test])

IP Addresses for Testing:

192.168.211.86

192.168.56.232

192.168.157.120

192.168.6.6

192.168.107.151

192.168.208.39

192.168.54.185

192.168.158.70

192.168.3.216

192.168.160.167

Source IP Address for Testing

192.168.1.132

Testing for Connection Failure Results:

Test IP:192.168.1.132 with IP:192.168.211.86: Failed Connection. See Packet 1064 as Reference Followed by Packet 1177 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.56.232: Failed Connection. See Packet 1065 as Reference Followed by Packet 1178 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.157.120: Failed Connection. See Packet 1066 as Reference Followed by Packet 1184 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.6.6: Failed Connection. See Packet 1067 as Reference Followed by Packet 1185 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.107.151: Failed Connection. See Packet 1068 as Reference Followed by Packet 1186 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.208.39: Failed Connection. See Packet 1069 as Reference Followed by Packet 1187 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.54.185: Failed Connection. See Packet 1070 as Reference Followed by Packet 1191 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.158.70: Failed Connection. See Packet 1071 as Reference Followed by Packet 1192 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.3.216: Failed Connection. See Packet 1072 as Reference Followed by Packet 1193 asking for a retransmission for Connection Failure.

Test IP:192.168.1.132 with IP: 192.168.160.167: Failed Connection. See Packet 1053 as Reference Followed by Packet 1172 asking for a retransmission for Connection Failure.