Name and Section: McKenzie Eshleman

1 Lab Preparation

- Download the following trace files to your working directory:
  - `icmp1.pcapng`
  - `icmp2.pcapng`

Submission

Submit all of your work in **neatly hand-written** or **typed** format.

What to turn in:
- The completed lab packet

2 Lab Assignment

- Open the trace file: `icmp1.pcapng` in Wireshark.

1. What is the display filter for ICMP? Apply the filter.

   The display filter to show ICMP, is simply icmp

2. What is the exact filter for an ICMP Echo Request message? Echo Response message? (*i.e field.name == x*)

   echo.request and echo.response

3. How did Wireshark ascertain that the data encapsulated within the IPv4 packet was was an ICMP message?

   Wireshark ascertains that the data encsapsulated within the IPv4 packet is ICMP by the protocol value that each packet has, for this specific file has protocol 1 (ICMP).

4. With respect to ICMP, explain what is happening in this trace? What command line tool that you have used would create this type of traffic?

   Traceroute most commonly uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values. The response time of each hop is calculated. To guarantee accuracy, each hop is queried multiple times (usually three times) to better measure the response of that particular hop. A command line tool that can be used for this specific kind of traffic is TRACERT which determines the route to a destination by sending ICMP echo packets to the destination.

5. What is the layer 2 address of the device that initiated the network traffic?

   The layer 2 address of the device that initiated the network traffic is the Address Resolution Protocol, used to translate between Layer 2 MAC addresses and Layer 3 IP addresses.

6. What are the ICMP ID values for each of the Echo Request messages? Why are there two values displayed in wireshark? ("LE" and "BE")

   The ICMP ID values for each Echo Request Message is type 8, which is a Echo (ping) request. There are two values being displayed in WireShark, these are the Identifier BE and LE. This simply means its is in Big Endian or Little Endian

7. What are the ICMP ID values for the Echo Response messages?

   The ICMP ID values for a Echo Response message is Type 0

8. What are the ICMP Sequence Number values for the Echo Request messages? List in hex format using the big endian value

   The ICMP Sequence Number values for the Echo Request Message is 1 and 256, in hex and BE this is a value of 0x0001.

9. What are the ICMP Sequence Number values for the Echo Response messages? List in hex format using the little endian value

   The ICMP sequence Number for a Echo Response Messafe is 1 and 256, where the hex value in BE is 0x0001

10. What can you deduce based on the answers to questions '7-9'?

    Based off of questions 7-9, we can deduce that the sequence number will remain the same , regardless on if the Echo message is a Request or a Response .

- Open the trace file: `icmp2.pcapng` in Wireshark.

11. What is the display filter for an ICMPv4 Time Exceeded - TTL Exceeded in Transit Message?

    The display filter for ICMPv4 is icmp.type == 11

12. Using the display filter for TTL Exceeded in Transit, you should have only TTL exceeded messages remaining. Why do the resulting packets have two ICMP messages encapsulated within them?

    The resulting packets have two ICMP messages encapsulated within them because The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram

- In Wireshark, make the following modifications to your column layout preferences
- Hide the columns; 'time', 'length', and 'info'
- Add custom columns for the ICMP type, ICMP code, and the useful version of the ICMP Sequence number.

13. What are the display filters for the new columns?

icmp.type == x

icmp.code == x

icmp.seq == x

- Hide the columns you just added, add a column to display the IPv4 id value

14. What is the display filter you used? What does this column provide that is helpful for identifying what is going on with the traffic?

The display filter used was ip.id, this column provides the information that can be used in for diagnostic to correlate datagrams measured at various locations along a network path.

3 Review Questions

15. What is the purpose of ICMP?

The purpose of ICMP is it is a transport level protocol within TCP/IP which communicates information about network connectivity issues back to the source of the compromised transmission

16. What was the `'ping'` tool originally designed for? What else is `'ping'` commonly used for?

Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from active sonar terminology that sends a pulse of sound and listens for the echo to detect objects under water.

17. What type of device might generate an ICMP Type 3, Code 13 message?

The type of device that might generate an ICMP Type 3, Code 13 message is a router. This can be from a response to a packet that is dropped because its forwarding is administratively prohibited.

18. You have captured only ICMP packets on your network. How can you determine what triggered the ICMP Type 11 packets you see in the traffic?

You can determine what triggered the ICMP type 11 packet by looking at the time it took to send the packets, since type 11 is code for a time extender.

19. What should an IPv4 router do when a packet arrives with a TTL value of 1?

An IPv4 router will have a period of 1, if it recieves a TTL value of 1. This is a sufficent value for TTL.