Christopher Bazyani

Practical Cyber Security

Unit 5

Packet Sniffing – ICMP

**Open the trace**

Opening the ICMP pcap file supplied

Graphical user interface, text, application

Description automatically generated

Examining one of the ping request packets sent by my host, I see the checksum, sequence number and identifier fields are two bytes each. The Checksum is listed below

Graphical user interface, application, table

Description automatically generated

**Echo (ping) Packets**

Selecting the first echo (ping) request and reply packet at the start of the trace



Expanding the ICMP block to see the ICMP header and payload details. The ICMP header starts with a Type and Code field that identify the kind of ICMP message. Looking to see the values for an echo request and an echo reply and how they compare.

A screenshot of a text message

Description automatically generated with low confidence

Graphical user interface

Description automatically generated

The Type/Code is followed by a 16-bit checksum over the complete ICMP message

Graphical user interface, text, application, chat or text message

Description automatically generated

Identifier and Sequence Number field. These fields are used to link echo request and reply packets together. Looking at the Identifier and Sequence Number values for several requests and replies

Text

Description automatically generated

Text

Description automatically generated

Lastly, there is a Data field as the ICMP payload

Text

Description automatically generated with low confidence

In both the echo reply and the request, the data is same. The echo request sender will use any data that is convenient, and the echo reply sender can copy the data from the request so that the payload is returned to the original sender.

**TTL Exceeded (traceroute) Packets**

Exploring traceroute traffic by selecting any Time Exceeded ICMP packet in my trace



Expanding the ICMP block to see the ICMP header and payload details

Graphical user interface, text, application

Description automatically generated

16-bit checksum over the complete ICMP message to check that it was received correctly

Text

Description automatically generated

ICMP header of the echo request packet

Text

Description automatically generated