Reexamine the fields of a packet header

While there are many different tools available to use, it's important as a security analyst that you learn how to read and analyze packets manually.
To do so, let's examine an important packet component: IP headers.

Previously, you learned about the four layers of the TCP/IP model.
Remember, the TCP/IP model is a framework that is used to visualize how data is organized and transmitted across a network.

The internet layer accepts and delivers packets for the network.
It's also the layer where the Internet Protocol operates as the foundation for all communications on the internet.
It's responsible for making sure packets reach their destinations.

The Internet Protocol operates like a mail courier delivering an envelope.
Instead of using the delivery information found on the envelope, the Internet Protocol uses the information found in a packet header, like IP addresses.
It then determines the best available route for packets to take, so that data can be sent and received between hosts.

As you may already know, IP packets contain headers.
Headers contain the data fields essential to the transfer of data to its intended destination.
Different protocols use different headers.

There are two different versions of the Internet Protocol: IPv4, which is considered to be the foundation of internet communications, and IPv6, which is the most recent version of the Internet Protocol.
Remember, different protocols use different headers.
So IPv4 and IPv6 headers differ, but they contain similar fields with different names.
IPv4 is still the most widely used, so we'll focus on examining the fields of an IPv4 header.

Let's start with the Version field, which specifies which version of IP is being used, either IPv4 or IPv6.
Referring back to our mail analogy, the Version field is like the different classes of mail, like priority, express, or regular.

Next, IHL stands for Internet Header Length.
This field specifies the length of the IP header plus any options.

The next field, ToS stands for Type of Service.

This field tells us if certain packets should be treated with different care.
For example, think of ToS like a fragile sticker on a mailed package.

Next is the Total Length field, which identifies the length of the entire packet, including the headers and the data.
This can be compared to the dimensions and weight of an envelope.

The next three fields, Identification, Flags, and Fragment Offset, deal with information related to fragmentation.
Fragmentation is when an IP packet gets broken up into chunks, which then get transmitted over the wire and reassembled when they arrive at their destination.
These three fields specify if fragmentation has been used and how to reassemble the broken packets in the correct order.
This is similar to how mail can travel through multiple routes like mailboxes, processing facilities, airplanes, and mail trucks before it reaches its destination.

The TTL field stands for Time to Live.
Like its name suggests, this field determines how long a packet can live before it gets dropped.
Without this field, packets could loop through routers endlessly.
TTL is similar to how tracking information provides details about an envelope's expected delivery date.

The Protocol field specifies the protocol used by providing a value which corresponds to a protocol.
For example, TCP is represented by 6.
This is similar to including the number of a house in a postal address.

The Header Checksum stores a value called a checksum, which is used to determine if any errors have occurred in the header.

The Source Address specifies the source IP address and the Destination Address specifies the destination IP address.
This is just like the sender and receiver's contact information found on an envelope.

The Options field is not required and is commonly used for network troubleshooting rather than common traffic.
If it's used, the header length increases.
It's like purchasing postal insurance for an envelope.

Finally, at the end of the packet header is where the packet's data resides, like the text in an email message.

Who knew that the packets of data we send across networks contain so much information?
Coming up soon, you'll have the opportunity to examine these packet fields in detail.

Revision #1
Created 2023-09-10 06:35:57 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai