Christopher Bazyani

Practical Cyber Security

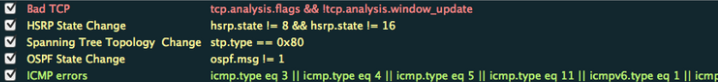
Unit 2

Packet Sniffing – Ethernet

Introduction Questions

**1. If a packet is highlighted by black, what does it mean for the packet?**

When a packet is outlined in black, it means that it has some serious issues. For instance, it could include stuff like packet errors, spanning tree topology changes, packets that can't be sent in order, and an open shortest path first state update.



**2. What is the filter command for listing all outgoing http traffic?**

We could use Wireshark's filtering feature by typing "http" in the filtering area to filter the connections that want a focus on all outgoing HTTP traffic.

**Text

Description automatically generated**

**3. Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?**

Since UDP is an inefficient connectionless protocol for applications who don't want TCP's sequencing or flow control and want to use their own, such as DNS, the DNS protocol uses the UDP stream. As a result, certain variables would need to use the DNS protocol's UDP stream. TCP is a secure connection-oriented protocol that allows a byte stream originating on one machine to be transmitted on another machine without error over the internet, such as HTTP. As a result, UDP is an unreliable connectionless protocol, whereas TCP is. This is the main distinction between them.

**4. Use Wireshark to capture the FTP password.**

Using Wireshark, attackers grab login passwords from users using the File Transfer Protocol, which is a plain text protocol. Attackers can quickly catch information utilizing it in Wireshark.

Ethernet Analysis Questions

**1. How long are the combined IEEE 802.3 and LLC headers compared to the DIX Ethernet headers? You can use Wireshark to work this out. Note that the Trailer/Padding and Checksum may be shown as part of the header, but they come at the end of the frame.**

The IEEE 802.3 header, like DIX Ethernet, is 14 bytes long. Both come with a trailer that includes a checksum and padding if necessary. LLC adds three more bytes of headers, bringing the number to 17 bytes.

**2. How does the receiving computer know whether the frame is DIX Ethernet or IEEE 802.3?**

The IEEE 802.3 length field and the DIX Ethernet Type field are in the same place. The value is perceived as a frame length if it is less than 0x600 (1536). The value is interpreted as a Type value if it is greater than 0x600 (1536).

**3. If IEEE 802.3 has no Type field, then how is the next higher layer determined? Use Wireshark to look for the demultiplexing key.**

To express the next higher layer protocol, IEEE 802.3 attaches the LLC header directly after the IEEE 802.3 header. Instead of the two bytes in the type field, LLC uses a single initial byte called the destination service access point (DSAP).