CS315 Computer Security

Lab Assignment1

Name | Yubin Hu
ID | 11712121
Date | 2020.09.07

Questions for the Lab

1. Carefully read the lab instructions and finish all tasks above.

   > omitted

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

   > Wireshark uses colors to help you identify the types of traffic at a glance.
   >
   > Black identifies TCP packets with problems. For example, thet could have been delivered out-of-order.

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

   > ```
   > 1 http
   > ```

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

   > DNS(UDP stream):
   >
   > - DNS(Domain Name System) is an application layer protocol.
   > - DNS primarily uses the UDP(User Datagram Protocol, transport layer protocol)
   > - The reason why does DNS use UDP:
   >   - UDP is much faster.
   >   - DNS requests are generally very small and fit well within UDP segments.
   >   - UDP is not reliable, but relibility can added on application layer.
   >
   > HTTP(TCP stream):
   >
   > - HTTP(Hypertext Transfer Protocol) is an application-layer protocol that runs over TCP.

- When a host requests a web page, transmission reliability and completeness must be guaranteed. Therefore, HTTP uses TCP as its transport layer protocol.

5. Using Wireshark to capture the FTP password.