Wireshark Practical

Introduction

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed. Wireshark is perhaps one of the best open source packet analyzers available today.

Here are some examples people use Wireshark for:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

Hands-on Wireshark

Capturing packets

Follow the given steps to capture a set of packet from the network.

1. Start Wireshark on your Linux machine by issuing the following command on a terminal.

   # sudo apt-get install wireshark

   # sudo wireshark

   Select the correct network interface and start capturing packets.

2. Open a web browser and go to different websites for a little time.
3. Ping from a new terminal to 8.8.8.8
4. Now, stop capturing packets in Wireshark and save the captured packets to a pcap file for later use.
5. Open the saved le from Wireshark once again and look at different packets by double-clicking on them.

Using Wireshark filtering

Wireshark provides a powerful packet filtering capability which can be used to isolate a specific packet, which meets a given criteria. Filter: text field on Wireshark window is the place where we can apply filters.

1. Enter following simple protocol names as filters and check whether such packets exists. Once you apply one filter, don't forget to click the clear button before applying another filter. Just deleting the text you entered does not clear the previous filter unless you click on the clear button.

   http , tcp , smtp , arp

2. Select ARP request and analysed it. Clearly mentioned about the MAC & IP address of sender and target.

3. Write down and apply a filter to view packets where the IP address 212.39.96.70 and the protocol is HTTP.

4. Analyze the first HTTP GET request under the HTTP header.a. What is the request version? b. What is the request URI

5. Analyze the server's response to the GET request.
   a. What is the status code?
   b. What does that status code mean?
   c. What is the value of the response phase?

6. Analyze the IP header of the same packet
   a. What is the IP version?
   b. What is the length of the header?
   c. What is the total length of the packet?
   d. Value of fragment offset?
   e. Value of Time to Live?
   f. Value of the header checksum?
   g. IP addresses of the source and destination?

Submission

Create a pdf document with your answer (screen shots if necessary) and upload it to the UGVLE.