Assignment 5: Packet tracer and traffic analysis with Wireshark.

Submission due: 25th-29th October 2021

Overview:

Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.

The Wireshark User Guide can be found at: http://www.wireshark.org/docs/wsug_html_chunked/

Capturing Packets

After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface.

Test Run

Do the following steps:

1. Start up the Wireshark program (select an interface and press start to capture packets).
2. When Wireshark is first run, a default, or blank window is shown. To list the available network interfaces, select the Capture->Interfaces menu option. To capture network traffic, click the **Start** button for the network interface you want to capture traffic on. Windows can have a long list of virtual interfaces, before the Ethernet Network Interface Card (NIC).
3. Generate some network traffic with a Web Browser, such as Internet Explorer or Chrome. Your Wireshark window should show the packets
4. To stop the capture, select the Capture->**Stop** menu option, Ctrl+E, or the Stop toolbar button. What you have created is a Packet Capture or 'pcap', which you can now view and analyse using the Wireshark interface, or save to disk to analyse later. The capture is split into 3 parts:
    a. Packet List Panel – this is a list of packets in the current capture. It colours the packets based on the protocol type. When a packet is selected, the details are shown in the two panels below.
    b. Packet Details Panel – this shows the details of the selected packet. It shows the different protocols making up the layers of data for this packet. Layers include Frame, Ethernet, IP, TCP/UDP/ICMP, and application protocols such as HTTP.
    c. Packet Bytes Panel – shows the packet bytes in Hex and ASCII encodings.

5. To select more detailed options when starting a capture, select the Capture->Options menu option, or Ctrl+K, or the Capture Options button on the toolbar. Some of the more interesting options are:
    a. Capture Options > Interface - Again the important thing is to select the correct Network Interface to capture traffic through.
    b. Capture Options > Capture File – useful to save a file of the packet capture in real time, in case of a system crash.
    c. Display Options > Update list of packets in real time – A display option, which should be checked if you want to view the capture as it happens (typically switched off to capture straight to a file, for later analysis).
    d. Name Resolution > MAC name resolution – resolves the first 3 bytes of the MAC Address, the Organisation Unique Identifier (OUI), which represents the Manufacturer of the Card.
    e. Name Resolution > Network name resolution – does a DNS lookup for the IP Addresses captured, to display the network name. Set to off by default, so covert scans do not generate this DNS traffic, and tip off who's packets you are sniffing.

    Make sure the MAC name resolution is selected. Start the capture, and generate some Web traffic again, then stop the capture.

Questions (Please take screenshots and explain**)**

1. **Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighboring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.**
2. **Generate some web traffic and**
    a. **find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.**
    b. **How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)**
    c. **What is the Internet address of the website? What is the Internet address of your computer?**
    d. **Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.**
    e. **Find out the value of the Host from the Packet Details Panel, within the GET command.**
3. **Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.**

4. **Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.**
5. **Filter packets with http, TCP, DNS and other protocols.**
    a. **Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button..click on follow**.
6. **Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.**
7. **What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?**
8. **What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?**
9. **Find the following statistics:**
    a. **What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?**
    b. **What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?**
10. **Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.**