COMP30660 - Computer Arch & Org (Conv) -2022/23

Assignment 4
Wireshark

Due 30th April 2023 by 23:59

The objective of this assignment is to give preliminary understanding about some important network protocols and the wireshark usage.

Please follow the below guidelines to create the PCAP file required to continue the assignment.

- Install wireshark in your computer
- Start wireshark and select the network adapter that you are using to access internet (eg: if you are currently access internet using WiFi, it is the WiFi adapter)
- Start packet capturing process of the selected network adapter.
  Before starting packet capturing, close all other operations with internet on your machine as much as possible. Wireshark captures all the packets through the selected network interface. Having a lot of network related operations will finally create a very large PCAP file that may finally affect the answers in the assignment.
- Open a new command prompt and execute following commands (Some of these commands might not work in UCD wireless WiFi. Please try using some other WiFi network)
  - Type *ping 8.8.8.8 -n 10* and press enter
  - After completing ping, type *nslookup www.ucd.ie*, and press enter
  - After completing nslookup, type *ftp ftp.sunet.se*, and press enter
  - Enter "*anonymous*" as the user name and password can be anything
  - Enter *quit* and exit the ftp session.
- Open a browser
  - Browse this url: http://respondto.it/
  - Close the tab and open a new tab
  - Browse this url: http://vbsca.ca/login/login.asp
  - Enter arbitrary username and password and press login button. Check the login status
  - Close the tab and open a new tab
  - Play a youtube video for around 2 minutes
  - Close the youtube tab
- Stop packet capturing and save the captured packets into a PCAP file. Then open the saved PCAP file to continue the assignment.

Provide short answers to all the questions below using the opened PCAP file and properties of your computer. You should complete this assignment individually and you should provide evidence such as wireshark screenshots for the questions, where applicable.

1) What is the IP address of the network interface that you selected? How did you check the IP address?

2) Fill in the following table using the details of the created PCAP file.

Parameter	**Value**
Time span, s	
Total packets in the capture	
Bytes, MiB	
Average packet size, B	
Average packets per seconds, pps	
Average bits per second, b/s	

3)
   a) What is the command for filtering all the packets received (inbound) to the selected interface?
   b) What is the command for filtering all the packets exited (outbound) from the selected interface?

4)
   a) Why do we use ping command?
   b) What is the underlying protocol related to ping?
   c) What is the wireshark filter for ping frames?
   d) How many packets can you see when you apply this filter?
   e) What is the reason for seeing more packets than ping requests (here we sent 10 requests)?
   f) How can we filter only ping request frames (sent 10 requests) using wireshark?

5)
   a) What is the usage of nslookup protocol?
   b) What is the filter that can be used to capture packets related to nslookup command execution for www.ucd.ie?

6)
   a) What is the functionality of ftp command?
   b) How to filter ftp packets in wireshark?
   c) How many packets can you see when you apply this filter?

7)
   a) How to filter frames related to http sessions?
   b) What is the IP address of the “respondto.it” url?
   c) In which header can you find the url of the “respondto.it”? (hint: filter packets related to this url query, select a packet, and explore it)
   d) What are the http methods that you can see when you apply the filter in part b?
   e) What is the protocol used to find the IP address corresponding to a domain name?

8)

a) Can you see any TCP frames in your pcap file? (hint: apply filter for TCP packets)
b) What is a three-way handshake in TCP?
c) What is the filter required to filter only TCP SYN frames?
d) What is the filter for identifying tcp packets that contain “vbsca”?
e) Where can you see your submitted username and password in a packet related to this filter?

9)

a) How to identify TCP packets which contains “youtube” in wireshark?
b) What are the different protocols that you can see when you apply this filter?
c) Explain the difference between one-way SSL (Secure Socket Layer) and two-way SSL.

10) Draw the IO graph related to this PCAP file.

You have to upload an answer sheet which is constructed as a single PDF file for these questions.

You should upload your created PCAP file into a drive and share the link in your answer sheet. You can delete this file after 15th May 2023. We randomly select some assignments and cross check the answers with the PCAP content.