CS422 Lab1: Wireshark and Traceroute

Due: 23:59:59 PM, Wed Jan 24, 2024
Updated on Jan 18, 2024
Total points: 50 points

1 Goal

You are going to install **Wireshark** and use it to capture data packets while you measure hop-by-hop delay via **traceroute**.

2 Before you start

1. Please download and install Wireshark (`https://www.wireshark.org`). If your computer does not support Wireshark, you can use `tcpdump`. The difference is that Wireshark supports UI while tcpdump not. Both can be used to capture and analyze packets for this lab.
2. Please learn how to use Wireshark (or `tcpdump`). You can find a lot of online resources useful, for example, Wireshark Cheat Sheet (e.g, https://www.comparitech.com/net-admin/wireshark-cheat-sheet/) and tcpdump cheat sheet (or `man tcpdump`).
3. You must work individually on this assignment. You can work on your computer or on the XINU machines (xinu1.cs.purdue.edu, xinu2.cs.purdue.edu, etc.) that are in HAAS 257 and remotely accessible.

3 Part A: Data collection (20 points)

Please run `traceroute` to the following destinations while turning on Wireshark (tcpdump) to capture packets. You need to start packet capturing before you run traceroute and stop packet capturing when traceroute stops.

Please run `traceroute` as follows:

```
traceroute -I [Destination, e.g., www.cs.purdue.edu]
```

Tip: You can do "man traceroute" to learn why we want to use "-I".

Please traceroute one of the following three destinations:

- Destination A (local in your state), e.g., www.cs.purdue.edu if you are at West Lafayette, IN,
- Destination B (popular in the US), e.g., www.google.com, www. amazon.com, to name many,
- Destination C (oversea), e.g., www.gov.uk, to name many.

  Tip: An IP address can be used as the destination if known.

For each destination (say, A, B, C), please save two files: (1) the printout of your traceroute as A.txt, B.txt, C.txt, and (2) its corresponding packet traces captured by wireshark as A.pcap, B.pcap and C.pcap.

Note: please reduce the volume of pcap files if they are too big (> 2MB.) You need to figure out how to filter out some packets which are not relevant to traceroute. Please make sure each pcap file < 2MB.

4 Part B: Answer Questions (20 points)

Q1: For destination A, please answer the following questions:

- (2 points) please show A.txt or its screenshot.
- (2 points) What is the number of hops to this destination? If you can't, please explain why not.
- (2 points) Please go to its pcap file, locate the records as the response from the first-hop router (hint: use the IP address of the routers on the way to locate the traces). Print only these records (or the screenshot using wireshark).
- (2 points) What is the average of the round trip delays to the first-hop router towards this destination? If you can't, please explain why not.
- (2 points) What is the average of the round trip delays to this destination? If you can't, please explain why not.

Q2: Please compare traceroute results to destination A and destination B, and answer the following questions:

- (3 points) Compare all the hops and have you seen any hop in common? If yes, please show these hops in common and explain why. If no, please explain why not.
- (3 points) Please go to their pcap files and locate the response from these intermediate routers which are over the common hops. *(Hint: use the IP address of the routers on the way to locate the traces).* Please print only these records (screenshots are also fine).

Q3: Please compare traceroute results to destination A and destination C, and answer the following questions:

- (2 points) please show C.txt or its screenshot.
- (2 points Can you locate the hop which is across the ocean in the traceroute results to destination C? If yes, please explain why and show the IP addresses of the involved router(s). If no, please explain why not.
- (2 points) Please running ”ping [ip-address]”, where ip-address is the one of the involved router. Please compare the ping results and traceroute results. Do you see that these round trip time is comparable? If yes, please explain why. If no, please explain why not.

Note: you will be unable to get the delay if it returns “* * *”. In this case, please try another destination or just tell us what you can measure and what you not.

5 Part C: Packet Trace Analysis (10 points)

Please write a program in Python or C to analyze the pcap file captured along with traceroute. (Hint: use ICMP to locate the packet records to/from the routers involved in the traceroute).

1. Please first generate hop.txt based on the output of traceroute. Each line is
   `hop k:  ip-of-router-at-hop-k`
   Please start with hop k = 1 till the last hop. ip-of-router-at-hop-k is the IP address of the router at hop k. For each hop k, please contain at most ONE router (pick the first one if there are more than one options). However, it is known that some routers at hop k are not visible (represented by *). In this case, it is impossible to analyze the relevant packets and generate the needed output. So you don't need to support any intermediate routers if they are not visible. For example, if all the routers at hop 3 are not visible, hop.txt will look like

   ```
   hop 1:  router-1
   hop 2:  router-2
   hop 4:  router-4
   ...
   ```

2. Please write a program called pcapTraceroute.py or pcapTraceroute.c to analyze the captured pcap file. Please run the program as follows:

   `python pcapTraceroute.py input.pcap hop.txt` (using Python)
   `pcapTraceroute input.pcap hop.txt` (using C).

   Here, input.pcap is the pcap file captured by wireshark and hop.txt is the above output hop results along with the same traceroute experiment.

   Your program will take hop.txt as the input and read it line by line and print the output result per line (as follows). Note that only one router is consider at each hop so that you need to extract the sendtime and recvtime of the FIRST probe to this router (if there are more than one probe). Please print the output of the program line by line with each line containing

   ```
   hop k:  ip-of-router-at-hop-k, sendtime, recvtime, interval
   ```

   Please start with hop = 1 till the last hop. ip-of-router-at-hop-k is the IP address of the router at hop k, sendtime is the timestamp of the ICMP packet sent by the source node to this router, recvime is the timestamp of the ICMP response from this router to the source, interval is the interval between sendtime and recvtime, in miliseconds (ms).

3. please test your program using data traces collected in Part A. Please feel free to write a script or manually generate hop.txt from A.txt (or B.txt, C.txt). hop.txt contains at most one line for each hop. For hop k without any visible router, please feel free to ignore it.

6 Materials to turn in

You will submit your assignment at **gradescope**. You submission should zip all the files into "lab1_UID*.zip", including the following files

1. **Files collected for Part A**: A.txt, B.txt, C.txt, A.pcap, B.pcap and C.pcap. Please make sure that wireshark packet traces (pcap files) each < 2MB. per each traceroute operation.

2. **Report (pdf or word) for Part B**. Please first include your name and UID. In the report, Please answer the above questions and paste the needed printouts in the right place (appendix is recommended).

3. **Program for Part C**.

7 Support

Questions about the assignment should be posted on Campuswire or asked during PSOs or office hours.