Assignment 1: Networking Tools and Wireshark

Deadline: January 20, 2025 EOD

SUBMISSION INSTRUCTIONS

Prepare a detailed observation and analysis report and the appropriate screenshots from the Wireshark and Terminal for listed questions with specific details asked in individual tasks. Submit your report in PDF format with <NAME>_<ROLL NO>_Report.pdf. Submit your wireshark traces named as <NAME>_<ROLL NO>_<QUESTION NO>.pcap. Zip all these files into a single zip file <NAME>_<ROLL NO>.zip and submit on MS Teams.

Part1: Networking Tools

This part aims to familiarize you with basic networking tools. *Read the man pages of the tools like* `ifconfig`, `ping`, `traceroute`, *and* `nslookup`.

1. Find the IP address of your machine, subnet mask, and network ID of your subnet.
2. Find the IP address associated with www.google.com and www.facebook.com using `nslookup`. Change the DNS server address in the `nslookup` command to the following four IP addresses: 172.16.1.164, 172.16.1.180, 172.16.1.165, and 172.16.1.166, and see whether the IP address of the above domain name (www.google.com) changes. If you see a change in the IP address of www.google.com, can you think of the reason behind the same?
3. Ping the IP address of one of your friend's machine IP within the software lab. Send the ping packets with different packet sizes (64, 128, 512 bytes) and timeout (100) for reporting packet loss percentage, min, avg, max, and stddev of round-trip time.
4. Run `traceroute` for www.google.com and print the summary. Count the number of hosts involved in the path from source to destination. Why do you see some "* * *" in the intermediate hops?

Report your observations in the submission PDF, along with the appropriate screenshots.

Part 2: Packet Analysis

This part of the assignment will familiarize you with the network sniffing and packet analyzer tool, Wireshark. It is an open-source and cross-platform tool. It is used for network troubleshooting, analysis, software, communications protocol development, and education.

1. **Analysis of DNS Packets: Structure and its Traffic**
   Use Wireshark to grab all packets on your wired interface while visiting the website

https://www.iitkgp.ac.in from your browser. Report the following:

a) Locate the DNS query and response messages. Is DNS using UDP or TCP in the observed packets?
b) Check the source and destination IP address of the DNS query.
c) How many DNS queries are sent from your browser (host machine) to DNS Server(s) during the name-to-IP resolution?
d) Which DNS Server replies with actual IP Address(es).
e) How many DNS servers are involved? Do all DNS servers respond?
f) Clearly list the resource records involved in resolving the site's IP address, mentioning Name, Type, Class, TTL, Data length, and resolved IP address appropriately in the complete resolving process of this DNS conversation, including query/queries and response/answer(s).

Provide appropriate screenshots from the terminal and Wireshark to answer the above questions in your report.

2. Web Traffic (HTTP)

Initiate web traffic for the web server- http://web.simmons.edu/~grovesd/ through the browser from your local machine and do the following list of tasks in Wireshark.

a) Filter the HTTP packets and observe traffic between the client and the web server.
b) Check the header of the HTTP packet and try to identify the HTTP request and response.
c) How many HTTP packets are exchanged between client and server to load an entire web page?

Provide appropriate screenshots from the terminal and Wireshark to answer the above questions in your report.

3. ICMP Traffic (Ping/Traceroute)

a) Run '`ping`' and '`traceroute`' commands to initiate ICMP traffic for your friend's machine and capture it through Wireshark. Inspect & crosscheck the Source and Destination IP address of captured ICMP packets.
b) Send a ping to an unreachable host (e.g., a host with IP 192.168.31.3 does not exist in the IIT KGP network) and analyze ICMP no-response packets.
c) Perform a '`traceroute`' operation for both reachable and unreachable hosts and prepare a brief report of your observation using Wireshark.

Provide appropriate screenshots from the terminal and Wireshark to answer the above questions in your report.

Marks Distribution

Part 1 (10x4=40)
Part 2 (20x3=60)