COMP 7003
Applied Computer Science, Network Security Applications Development Option
September 2024

This is an individual assignment.

Objective

- This assignment aims to gain a deep understanding of TCP protocol operation, focusing on session management, data identification, and performance optimization mechanisms.
- This exploration will be achieved through Wireshark analysis and manipulation tools like curl, ncat, etc.
- Fundamentally, the purpose of the assignment is for you to get a deep understanding of how TCP works.

Learning Outcomes

- Analyze TCP session initiation and termination processes.
- Compare and contrast TCP/IP packet structures across different scenarios.
- Understand and explain the impact of TCP mechanisms on data transmission.
- Utilize network analysis tools to dissect network traffic.
- Demonstrate knowledge of network performance metrics and recovery mechanisms.

Details

Flags

- Use hping3 to set each flag (a different packet per flag).
- Be sure to show the hping3 command and the wireshark screenshot that shows the flag being set.

Start and End of a Session

- Using Wireshark, capture a TCP session (e.g., send “hello” using ncat).
- Identify and explain the role of SYN and FIN flags in marking session start and end.
- Provide screenshots of relevant packets.
- What is the total number of bytes sent in the transfer? Explain how you determined that from the Wireshark data.

Same Data, Different Packets

Within a Session

- Send the same data twice within the same session (e.g., send “hello” twice).
- Compare IP and TCP header fields using Wireshark filters.
- Identify and explain differences in fields like sequence numbers, acknowledgment numbers, etc.
- Provide screenshots and detailed explanations.
- ncat is helpful for this.

Across Sessions

- Send the same data in two separate sessions (e.g., send “hello” in one session and then “hello” in the second session).
- Compare IP and TCP header fields.
- Explain differences in source/destination ports, sequence/acknowledgment numbers, flags, etc.
- Provide screenshots and explanations.
- ncat is helpful for this.

Website Download and TCP Analysis

- Download a book from Project Gutenberg using a browser.
- Capture the download packets with Wireshark.
- Analyze captured data, focusing on slow start and fast recovery phases.
- Identify features like initial window size increase, congestion window adaptation, and fast retransmission.
- Generate and explain graphs:
    - Throughput (Mbps) over time
    - Window size (bytes) over time
    - Congestion window (bytes) over time
    - Cumulative number of retransmissions over time
    - Retransmission graph

Constraints

- Follow the guidelines.
- Adhere to ethical guidelines and respect network resources.
- Use clear and concise language in your report.
- Cite any external sources used.

Resources

- Wireshark documentation and tutorials
- Man pages for tools like curl, ncat, etc.
- Online resources on TCP and performance analysis

Submission

- Follow the assignment submission requirements.
- Be sure you are aware of the late submission policy.

***Note:** Please strictly adhere to the submission requirements to ensure you don't lose any marks.*

Evaluation

Topic	Value
Flags	10
Session Start/End	10
Same Session	25
Different Session	25
Website Download (graphs etc…)	20
Clarity/Completeness	10
Total	**100**

Hints

- Refer to the online resources and tutorials for tool usage and data interpretation.
- Organize your report systematically, outlining findings clearly.
- Double-check your explanations and ensure they are technically accurate.