Network Monitoring Reflection (Task 4)

Date: 2025-09-29

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Course/Section: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1) Why is it important to monitor active connections on a server, especially during a potential attack?  
  
Answer:  
-   
-   
-

2) Which MySQL connection(s) did you observe (addresses/state/PID)?  
  
Answer:  
-   
-

3) If you terminated a (simulated) malicious connection, what was the PID and what evidence supported that decision?  
  
Answer:  
-   
-

4) Discuss the significance of identifying and terminating malicious connections. What are the risks of terminating the wrong PID, and how can disruption be minimized?  
  
Answer:  
-   
-

5) List two best practices for ongoing network monitoring and incident response.  
  
Answer:  
-   
-

Attach screenshots or include snapshots from lab\_outputs/.