```
In [ ]: Training Day 16 Report– 8 July 2025
         Introduction
         Day 16 introduced low-level exploit concepts, particularly buffer overflows a
         safety issues. The session focused on why memory corruption vulnerabilities a
         how mitigations work.
         Key Concepts Discussed
         We explored stack vs heap memory, how input validation errors can overwrite c
         structures, and the defenses such as ASLR, DEP/NX, and stack canaries that co
         modern exploitation.
         Lab Preparation in Theory
         A safe exercise plan was described for compiling intentionally vulnerable pro
         toggling compile-time protections to observe differences in behavior. The cla
        sized non-production environments for such work.
         Practical Understanding (Theory)
         We discussed ethical considerations for exploit development and why understan
        fensive techniques is necessary for realistic testing. The trainer also outlin
         document findings responsibly.
         Key Takeaways
         Memory vulnerabilities require specialized knowledge; working in lab environm
         respecting boundaries is essential.
         Conclusion
         Following memory concepts, the next session will cover exploitation framework
        exploitation workflows.
```