

Lecture 23: May 22, 2026

Reading: *text*, §24.2–24.2

Due: Homework 4, due May 27, 2026

1. Greetings and felicitations!
2. Penetration Studies
 - (a) Goals
 - (b) Where to start
 - i. Unknown system
 - ii. Known system, no authorized access
 - iii. Known system, authorized access
3. Flaw Hypothesis Methodology
 - (a) System analysis
 - (b) Hypothesis generation
 - (c) Hypothesis testing
 - (d) Generalization
4. System Analysis
 - (a) Learn everything you can about the system
 - (b) Learn everything you can about operational procedures
 - (c) Compare to other systems
5. Hypothesis Generation
 - (a) Study the system, look for inconsistencies in interfaces
 - (b) Compare to other systems' flaws
 - (c) Compare to vulnerabilities models
6. Hypothesis testing
 - (a) Look at system code, see if it would work (live experiment may be unneeded)
 - (b) If live experiment needed, observe usual protocols
7. Generalization
 - (a) See if other programs, interfaces, or subjects/objects suffer from the same problem
 - (b) See if this suggests a more generic type of flaw
8. Elimination
9. Examples
 - (a) Michigan Terminal System
 - (b) Burroughs B6700 System
 - (c) Corporate computer system