Lecture 5: April 7, 2021

Reading: *text*, §24.2

Assignments: Homework 1, due April 7, 2021
Lab 1, due April 19, 2021

1. Penetration Studies
   (a) Goals
   (b) Where to start
      i. Unknown system
      ii. Known system, no authorized access
      iii. Known system, authorized access
2. Flaw Hypothesis Methodology
   (a) System analysis
   (b) Hypothesis generation
   (c) Hypothesis testing
   (d) Generalization
3. System Analysis
   (a) Learn everything you can about the system
   (b) Learn everything you can about operational procedures
   (c) Compare to other systems
4. Hypothesis Generation
   (a) Study the system, look for inconsistencies in interfaces
   (b) Compare to other systems' flaws
   (c) Compare to vulnerabilities models
5. 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
6. 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
7. Elimination
8. Examples
   (a) Michigan Terminal System
   (b) Burroughs B6700 System