Outline for March 4, 2008

Reading: text, §17.2, 22.1–22.5

Discussion Problem. What do you think of the following homework assignment?

This is not an assignment for this class. I am only asking what you think of it. The assignment is reported on the web at http://isc.sans.org/diary.php?storyid=1155. The following is the entire assignment, verbatim. It was worth 15% of the grade.

> **The TASK**
>
> Student is to perform a remote security evaluation of one or more computer systems. The evaluation should be conducted over the Internet, using tools available in the public domain.
>
> **What the student must submit**
>
> In conducting this work, you should imagine yourself to be a security contracted by the owner of the computer system(s) to perform a security evaluation.
>
> The student must provide a written report which has the following sections: Executive summary, description of tools and techniques used, dates and times of investigations, examples of data collected, evaluation data, overall evaluation of the system(s) including vulnerabilities.

Lecture Outline

1. Isolation (con't)
   a. Sandboxes
2. Malicious logic
   a. Trojan horses, replicating Trojan horses
   b. Computer viruses: boot sector, executable infectors; multipartite; TSR; stealth; encrypted; polymorphic; macro
   c. Computer worms
   d. Bacteria and logic bombs