Lecture 9 Outline

April 26, 2016

Reading: *text*, §23 (except 23.6); [Nac97] **Assignments due:** Homework 3, on May 9

1. Greetings and felicitations!
   a. Midterm is Tuesday, May 2, in class
   b. Homework 3 is available and is due in 2 weeks, on May 9.
   c. I am cancelling my Wednesday 9am office hour; instead, I will hold one at 4:10pm today.
2. Puzzle of the Day
3. Types of malicious logic
   a. Quick review: Trojan horse
   b. Computer virus
      i. Boot sector infector
      ii. Executable infector
      iii. Multipartite
      iv. TSR (terminate and stay resident)
      v. Stealth
      vi. Encrypted
      vii. Polymorphic
      viii. Metamorphic
      ix. Macro
   c. Computer worm
   d. Bacterium, rabbit
   e. Logic bomb
   f. Keystroke logger
   g. Ransomware
   h. Botnets

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

> **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.

Important note: 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`.