Outline for January 13, 2003

Reading: Text, §23.1–23.2

Discussion Problem

What is suspicious about the following “ls” output?

```
host % ls -sail /var/mail
271873    1 drwxrwxrwt   3 root          512 Feb 21 12:26 ./
  3776    1 drwxrwxr-x  20 root          512 Aug 19  1996 ../
275649    1 drwxrwxr-x   2 root          512 Sep 11 12:43 :saved/
272086    0 -rw-rw----   1 ann             0 Feb 21 12:36 ann
272088    1 lrwxrwxrwx   1 bob            32 Feb 21 10:23 bob -> /etc/passwd
272087    4 -rw-rw----   1 bob          3515 Feb 21 12:23 cheryl
```

Outline for the Day

1. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
2. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems’ flaws
   c. Compare to vulnerabilities models
3. 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
4. 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
5. Peeling the Onion
   a. You know very little (not even phone numbers or IP addresses)
   b. You know the phone number/IP address of system, but nothing else
   c. You have an unprivileged (guest) account on the system.
   d. You have an account with limited privileges.
6. Example Penetration Studies
   a. Michigan Terminal System
   b. Burroughs System
   c. Attacking the Organization Directly