Outline for December 3, 2003

Reading: Chapter 23.2–23.4

Discussion Problem

Here's a little quiz to inspire you when you study for the final.

1. How long did the Hundred Years War last?
2. In which country are Panama hats made?
3. Where does catgut come from?
4. What is a camel's hair brush made of?
5. What kind of creatures were the Canary Isles named after?
6. What was King George VI's first name?
7. What color is a purple finch?

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
7. Vulnerability Models

And Their Answers

1. 116 years (from 1337 to 1453).
2. Ecuador.
3. From sheep and horses.
4. Squirrel fur.
5. A large breed of dogs. The Latin name was *Insularia Canaria* - "Island of Dogs."
6. Albert. When he came to the throne in 1936 he respected the wish of Queen Victoria that no future king should be called Albert.
7. The distinctively colored parts are crimson.

Courtesy of Peter Langston via the YUCKS digest.