Quiz 7, IS2935, Nov 20, 2003

Name :

---

1. State what the following mean. (4)

   Stealth virus: It can conceal infection. For example, it can trap a read access to provide disinfected file, whereas upon an execute call, it will send an infected file

   Trojan horse: It is a program that has an over and a covert effect, i.e. it appears to be doing normal, expected task, but is actually violating some security policy (such information leakage)

   False positive and false negative: False positive means the a normal activity is considered as an intrusion/attack by an IDS; False negative means, the IDS fails to recognize an intrusion/attack.

   Buffer overflow: Buffer overflow problem/vulnerability indicates that there is a possibility that an input to a variable is bigger than the variable can hold and this fact is not checked.

2. Describe flaw hypothesis method for penetration analysis? (3)

Answer: (refer to the slides for details)
Once information on system and environment has been gathered, flaws are hypothesized, which are then tested for. If the flaws are found, then they are generalized.

3. Note that the program *xterm* runs as root (with all the system privileges). As a solution to restrict any user running *xterm* and hence using root privileges to initiate malicious activities, the following check is done when *xterm* writes to the log_file – i.e., the process checks if the user running the *xterm* program can access the log_file; if yes then the log_file is opened for writing.

```
if (access("log_file", W_OK) == 0)
        fd = open("log_file", O_WRONLY|O_APPEND)
```

   Discuss how vulnerability class "race-condition" can be used to attack *xterm* program. Provide your answer on the back side. (3)

   Answer: Between the check for the condition and the open statement, if we execute a command that creates a symbolic link from "log_file" to a system file (e.g., a password file), then the race condition occurs. If that is done, now the user executing xterm can access information in the system file to attack the system