

Homework #1

Due date & time: 1:30pm on September 6, 2007. Hand in at the beginning of class (preferred), or email to the TA (zmao@purdue.edu) by the due time.

Late Policy: Late homeworks will not be accepted.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required. (2) Problem 2 requires you to start at least one week before it is due.

Problem 1 (5 pts) Do you currently use any computer security control measures on your computer(s)? If so, what? Against what attacks are you trying to protect?

Problem 2 (15 pts) Go to security focus mailing list website (<http://www.securityfocus.com/archive>), and subscribe to the bugtraq mailing list and at least one other mailing list there. Subscribe for at least one week, read the messages, and write down what you have learn from this experience. You could write a detailed description of one vulnerability reported in the mailing list, your sense of what are the common vulnerabilities, or any other thing.

Problem 3 (10 pts) Find a recent (2006 or 2007) computer security incidence that has been reported in the media, and analyze the incidence. For example, what was the main vulnerability that was exploited, what security principles were violated, what could have done to prevent the incidence, etc.

Problem 4 (30 pts) What permissions are necessary and sufficient to perform the following operations under UNIX operating systems? For example, to read the file `/d1/d2/f3`, one needs `x` on `/`, `x` on `/d1`, `x` on `/d1/d2`, and `r` on `/d1/d2/f3`.

1. write the file `/d1/d2/f3`
2. delete the file `/d1/d2/f3`
3. execute the file `/d1/d2/f3`, which is a binary file
4. execute the file `/d1/d2/f3`, which is a shell script
5. list the file names under the directory `/d1/d2s`
6. delete the directory `/d1/d2`, where the directory is empty
7. delete the directory `/d1/d2`, where `/d1/d2` contains one file `/d1/d2/f3`
8. delete the directory `/d1/d2`, where `/d1/d2` contains a subdirectory `/d1/d2/d3`, which contains one file `/d1/d2/d3/f4`
9. create the directory `/d1/d2/d3`, when `/d1/d2` exists, and `/d1/d2/d3` does not
10. rename a file from `/d1/d2/f3` to `/d1/d2/f4`

11. create a hard link /d1/d2/f3, which points to /d4/f5
12. remove /d1/d2/f3, which is a hard link pointing to /d4/f5
13. create a symbolic link /d1/d2/f3, which points to the directory /d4
14. read the file /d1/d2/f3/f5, where /d1/d2/f3 is a symbolic link pointing to the directory /d4, and /d4 contains a file /d4/f5
15. delete the file /d1/d2/d3/d5, in the same setting as above

Problem 5 (40 pts) Read Chapter 3 of Security Engineering and “Authentication in an Internet Banking Environment” by Federal Financial Institutions Examination Council (available from the handout page).

1. Write a set of guidelines on how users use passwords for an online bank. The guidelines should cover how the passwords are chosen, used, and updated.
2. Analyze the authentication technologies listed in the appendix of “Authentication in an Internet Banking Environment” and their pros and cons when applied to online banking.