

HOMWORK 3

ENTS 689i Network Immunity Fall 2008

Instructions

This assignment is **NOT** a group assignment. Each student should turn in their own set of answers. You should not collaborate for this assignment.

Answer each of the following questions and send your responses in ASCII (.txt) or PDF format to **npetroni@cs.umd.edu** no later than **12:01am EDT on October 27th, 2008 (midnight Sunday night)**. All other formats will receive **NO CREDIT**. Any mail arriving later than 12:01am on Monday morning (as determined by my mail server's time stamp) will be considered late. The standard course grading policy will apply for late homework on this assignment. If you turn in several copies of this assignment, the last one received will be graded and all others discarded.

Questions

1. (10 points) Pfleeger, Chapter 4, exercise 12.
Note that this problem refers to *access directories* and not Unix filesystem directories.
A directory is also an object to which access should be controlled. Why is it not appropriate to allow users to modify their own directories?
2. (20 points) Pfleeger, Chapter 4, exercise 22.
 - a) (5 points) If passwords are three uppercase alphabetic characters long, how long (that is, how much time) would it take to determine a particular password, assuming that testing an individual password requires 5 seconds?
 - b) (5 points) Argue for a particular amount of time as the starting point for "secure." That is, suppose an attacker plans to use a brute force attack to determine a password. For what value of x (the total amount of time to try as many passwords as necessary) would the attacker find this attack prohibitively long?
 - c) (10 points) If the cutoff between "insecure" and "secure" were x amount of time, how long would a secure password have to be? State and justify your assumptions regarding the character set from which the password is selected and the amount of time required to test a single password.
3. (12 points, 2pts each) Pfleeger, Chapter 5, exercise 5.
Can a user cleared for `<secret;{dog, cat, pig}>` have access to documents classified in each of the following ways under the military security model?
 - a) `<top secret;{dog}>`
 - b) `<secret;{dog}>`

- c) <secret;{dog,cow}>
 - d) <secret;{moose}>
 - e) <confidential;{dog,pig,cat}>
 - f) <confidential;{moose}>
4. (28 points, 4pts each) A group of students have accounts on a standard Unix system. All students are members of the group `students` and have accounts named `student1`, `student2`, etc. There are also a number of non-student users on the system who are not members of the group `students`. The following are a set of directory listings from the system:

```

/home/student1
-rw-r--r--      student1  students  myhomework.txt
-rwxr-xr-x      student1  students  mygame.exe
drwx-----    student1  students  secret

```

```

/home/student1/secret
-rw-----    student1  students  mysecretkey
drwxrwxrwx    student1  students  mydiary.txt

```

```

/home/student2
-rw-----    student2  students  myhomework.txt
-rwSr-x---    student2  students  mygame.exe

```

Assuming that students all have read and execute (but not write) permissions for each other's home directories, answer the following questions:

- a) Can student2 read student1's homework?
 - b) Can student1 read student2's homework?
 - c) Can student2 read student1's secret key?
 - d) Can student2 modify student1's diary?
 - e) Can student2 execute student1's game program? If so, with what user and group permissions will that process execute?
 - f) Can student1 execute student2's game program? If so, with what user and group permissions will that process execute?
 - g) Can non-students execute student2's game program? If so, with what user and group permissions will that process execute?
5. (10 points) Briefly explain (1-2 paragraphs) what code authentication is and how it can help with the Trojan problem.
6. (10 points) Briefly explain (~1 paragraph) what a runtime packer is. Explain (1-2 paragraphs) how and why some malicious software use runtime packing techniques.
7. (10 points) Explain (2-3 paragraphs) the difference between virus scanning and integrity verification. What are the relative advantages and disadvantages of each?