

## COSC 6397 Computer and Network Security

Computer Science Department, University of Houston, Instructor: Rakesh Verma

Spring 2008, Homework 3, Due April 16, 2008 at 5.00pm in my office (no email accepted)

Keep an organized Excel log of the time spent on each problem, and turn it in with the homework.

1. Read the paper “Know Your Enemy: Sebek2” and prepare two summaries of the article. One summary should consist of exactly 100 words from the article. The other summary should be in your own words and no more than 10 sentences. Should such articles be posted on the internet? Justify your position in at most half a page.
2. In the UNIX password scheme a salt is included to increase the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, those characters are known to everyone and need not be guessed. How exactly does the salt increase security? Would it be possible to dramatically increase the password security by increasing the salt size to say 48 bits?
3. Design a worm *on paper* that is controllable by you the developer. It should be designed so that you can control the extent to which it spreads. For example, a single host, a hundred hosts, a university site, and so on. Note: this is a paper design only - do **NOT** spread the worm.

Academic Honesty Policy: No collaboration with anyone or anything in or outside the course is allowed on any homeworks, exams and programming assignments (yes, that excludes the internet as well) except if it is **explicitly allowed** on a problem. The *appropriate* help of the instructor and (if applicable) the TA is of course allowed and encouraged.