CS 491/591 Spring '09 Test 4

Name:_____

This is a take-home test, **due Friday May 8th at the beginning of class,** turned in to either myself directly or to the ITV proctor (or via email, but the timestamp in my gmail account must say that it was received before the beginning of class on Friday). This is open Google, open book, open notes, open test keys, open everything. You may talk to your classmates or other people about the questions and ideas for answers, but you must state underneath the answer for that question erverybody who you talked to or worked with on that question, and your answer must be your own (both in terms of the writing, and the underlying ideas of the answer must be ideas that you at least contributed to).

You can email questions directly to me (jedcrandall@gmail.com), if I can answer them I'll answer and cc: secpriv-chat. Questions need not be about the test logistics, they can be about the material, but I'll have to decide how to answer each without giving the answer away, though. Feel free to bounce answers off of me and I'll let you know how I would grade them. You should know that 20s will be extremely hard to get, you need to teach me something to get a 20 on a question.

You can type your answers, or print this and write them, or anything you like as long as it's clear which answers correspond to which questions.

All questions are worth 20 points max. You get 18 points just for even attempting to answer the question. The other 2 points are subjective and based on how your answer reflects what you have learned in the lab and lectures this year.

Your answers should be five sentences minimum. You'll get 19 points if you give an excellent answer to a question, and 20 points if your answer includes some insight or idea that surprises me.

#1. In lab 2, we saw an example of how "information only has meaning in that it is subject to interpretation." A magic number (58623) was first interpreted as a signed 16-bit integer (-6911) to check the array bounds, then as an unsigned integer (58623) as the amount of data to read in a buffer. Then after the buffer was overflowed, this 16-bit data value was interpreted as the machine code for JMP ESP (0xff 0xe4) to jump to the stack pointer. In fact, in your lab2exploit.c code the data started out as an ASCII string (0x35 0x38 0x36 0x32 0x33) which was interpreted as input into an unnamed pipe and became part of a TCP/IP socket payload, *etc.*, so the same data was interpreted in dozens of ways during your exploit.

Name another example of information "only having meaning in that it is subject to interpretation" that came from another lab besides lab 2. It has to be another lab, something we talked about in lecture will not be accepted as an answer.

#2. Von Clausewitz said, "Where two ideas form a true logical antithesis, each complementary to the other, then fundamentally each is implied in the other. If the limitations of our mind do not allow us to comprehend both simultaneously, and discover by antithesis the whole of one in the whole of the other, each will nevertheless shed enough light on the other to clarify many of its details. In consequence we believe that the earlier chapters about defense will have sufficiently illuminated the aspects of attack on which they touch. But this is not always so. No analytical system can ever be explored exhaustively. It is natural that, where the antithesis does not lie so close to the root of the concept as in the previous chapters, what we can say about attack will not follow directly from what was said there about defense. A shift in our viewpoint will bring us nearer the subject, so that we can examine more closely what we previously surveyed from a distance. This will supplement our previous analysis; and what will now be said about attack will frequently also cast more light on defense."

(This is the intro to the part of the book that is about attack, which comes right after the part that is about defense.)

In the context of computer and network security, name something about defense that you have learned more details about by carrying out the attacks in one of the labs. Your answer should relate directly to one of the labs.

#3. Randy Browne, in his paper on the Turing Test for Information Flow, defined entropy to be "mathematical uncertainty about the definition of a system," rather than true uncertainty. In your opinion, would it be possible to build a system that enforces the Bell-LaPadula model of confidentiality and stops all forms of information leaks that violate policy, including <u>all</u> covert channels. Your answer should relate to Randy Browne's definition of entropy in some meaningful way.

#4. There are two important concepts (actually, there are many, but these are two of the most important ones) that we can learn from Claude Shannon: (1) The purpose of communication is to affect the behavior of the receiver, and (2) the information capacity of a channel is quantitatively equivalent to the receiver's uncertainty of the signal that will be received.

What do each of these concepts have to do with nmap and lab 3?

#5. What do Internet censorship and Metalica's music have to do with each other (other than that both of these things keep getting worse)? You can relate some concept in music to TCP/IP filtering and talk about interactions between multiple layers of abstraction. Or you can discuss Metalica's advocacy against pirated music and Napster, and how Digital Rights Management is or is not a form of censorship. This question is open ended but your answer needs to be serious, silly answers will not be accepted. Bonus point if you directly tie your answer into a specific song from Metallica's good (*i.e.*, pre-1990) albums.