**Print FAMILY name, first initial:**_____

# Examination 1

CEN 5540 Computer and Network Security
11 October 2005

**Instructions Read all instructions. Failure to follow instructions will result in loss of points.**

1. This is a closed-book examination.
2. You are permitted one 8.5 by 11 inch sheet of notes, both sides, that you have prepared.
3. You are permitted 90 minutes to complete this examination.
4. **Do not start** the exam until the proctor has told you to start.
5. **Answer the first question, and two more questions.**
6. **Answer any two (2) optional questions, and no more.** All optional questions are of equal value.
7. **Leave sufficient room in the upper lefthand corner for the staple** and staple your answer sheets in the room you have left.
8. Start the answer to each question on a new page (i.e., do **not** put the answer to more than one question on the same page).
9. Use exactly one page of paper (both sides is OK) to hold the answer to each question, and please write legibly.
10. Put the question number in the top center of each answer page and label each part of the question answer.
11. Show your work.
12. Include your last name and page number in the upper right hand corner of each answer page.
13. Assemble your answers in numerical order of the questions when you submit them.
14. Print your family name and first initial in the upper right hand corner of this page, and complete the honor statement affirmation below.

**Read and sign the following statement.** This page **MUST** be attached to your examination answers and **MUST** be completed to obtain credit for this examination.

On my honor, I have neither given nor received unauthorized aid on this examination.

Signed:

Printed Name:

SSN:

MANDATORY QUESTION

1. (a) (5) Analyze the code fragment below, and report any problems you can identify with its apparently intended operation, and how these (if any) can be corrected.

```
#include <unistd.h>
#include <fcntl.h>
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>

int main()
{
   int sock, bytes_recieved, fromlen;
   char buffer[65535];
   struct sockaddr_in from;
   struct in_addr address;
   sock = socket(AF_INET, SOCK_RAW, IPPROTO_RAW);
   fcntl(sock, F_SETFL, O_NONBLOCK);
   while(1)
   {
     fromlen = sizeof from;
     bytes_recieved = recvfrom(sock, buffer, sizeof buffer, 0,
                          (struct sockaddr *)&from, &fromlen);
     if(bytes_recieved != -1)
     {
       printf("\nBytes received ::: %5d\n",bytes_recieved);
       printf("Source address ::: %s\n",inet_ntoa(from.sin_addr));
     }
   }
}
```

   (b) (10) Explain how you performed OS fingerprinting. What did you use to distinguish various OSs? Which ones could you identify? Where did you get the information that formed the basis for this?

   (c) (5) What part of project 1 was most challenging for your team to develop? Why?

   (d) (5) What did you learn from project 1? Explain.

OPTIONAL QUESTIONS - ANSWER ANY TWO

2. (a) (10) Consider the security goal of integrity. Describe three different things that the term integrity could mean, and give a context in which they would be important.

   (b) (15) For each integrity definition above, describe a suitable control for it, how the control would work, and how it maintains the desired integrity.

3. (a) (4) Define the term computer worm, and distinguish from computer virus.

   (b) (9) Describe the typical operation of a computer worm for a complete life cycle. Give examples of how it might perform each of the steps in its life cycle.

   (c) (6) Describe the forms of loss that can be attributed to a computer worm, and their significance.

   (d) (6) Describe three controls for computer worms, how they are effective, and their pros and cons.

4. (a) (5) How do biometric authentication systems work, generically?

   (b) (10) What are advantages and disadvantages of BA systems? Explain.

   (c) (5) The acceptance threshold of a BA system is often chosen at the point where the False Accept Rate (FAR) is equal to the False Reject Rate (FRR). Why is this often done, and when should the threshold be chosen differently? Give examples.

   (d) (5) Describe a system in which biometric authentication could be combined with another, distinct authentication mechanism. What advantages does this system offer? For what applications is it appropriate?

5. (a) (9) From the following list of software engineering methods to promote system quality, which two are the most effective?

      i. live running the system
      ii. black box testing
      iii. white box testing
      iv. code inspection
      v. design inspection
      vi. requirements inspection
      vii. acceptance testing

      Why do you think these are more effective at finding faults than the other methods?

   (b) (8) What is configuration management, and why is it important? What are requirements for doing it, and why?

   (c) (8) What is cleanroom development, and what are its benefits?