Examination 2
Computer and Network Security
9 December, 1994

Instructions:

- Do not start until given permission to do so.
- Answer any four (4) questions below (graduate students may not answer question 1 and must answer the last question).
- Start the answer to a new question on a new piece of paper (that is, no more than one answer per page).
- Be sure to include your name on your answer sheets.
- This test is closed book, but you may use one 8.5 by 11 inch sheet of notes.
- You have 50 minutes to complete this examination.

1. Define and distinguish the following terms:
   (a) Back Door.
   (b) Logic Bomb.
   (c) Virus.
   (d) Worm.
   (e) Trojan Horse.
   (f) Bacterium.
2. (a) What sorts of logfiles are kept in Unix?
   (b) Why is ps(1) more accurate but slower than who(1) or users(1)?
   (c) What is syslogd and what does it do?
   (d) What kinds of information is it unwise to log, and why?
3. (a) Give a legitimate reason for a back door, and describe a control for detecting the presence of one inserted by an intruder.
   (b) Give a legitimate use for logic bombs.
   (c) Why aren't viruses the problem on Unix machines that they are on PCs?
   (d) Describe two controls for viruses.
4. (a) What must be protected by an operating system and why?
   (b) Describe two ways to protect main memory.
   (c) Compare access control lists and capabilities. How does Unix use these?
   (d) What are SUID and SGID programs and why are they dangerous?
5. (a) What are the two major differences between rlogin and telnet?
   (b) How can accounts be broken when these are used?
   (c) What are the host.equiv and the .rhosts files, and how are they different?
   (d) Why do .rhosts files drive system administrators crazy?
   (e) How can finger(1) be a vulnerability?
6. (a) What are 'trusted ports' and why shouldn't they be?
   (b) What are firewalls intended to do?
   (c) How do firewalls work?
   (d) How should a firewall be set up (which files/services should be on the firewall and which should not be)?
7. (a) What were the three approaches used by the Morris Internet Worm to attempt to infect another machine?
   (b) What were the underlying causes of these vulnerabilities it exploited?
   (c) Describe three ways in which the worm attempted to disguise or hide information.