Rubric for Homework #4

- Problems 1-6 worth 5 points
- Problems 7-8 worth 10 points

- Check along left side means earned all points for the problem
- Total minus points for a problem is along left side of page

Answers not labeled clearly: -1 overall (e.g. Problem 1 : R-1.12)
Low Readability: up to -3 per question
Lack of Clarity: up to -3 per question
Missed/wrong ideas or facts: -1 per idea/fact
Answer too long: up to -2 per question

If minus points not accompanied by a label, they are for missing ideas/facts. Wrong facts/ideas might be underlined.

Problem 1 : R-4.1

- insider attack
- Trojan horse (might be stretching it a bit)

Problem 2 : R-4.3

- take up computing resources: CPU time, disk space, system memory
- could over-replicate, thereby overloading systems
- upon being detected by an antivirus program, creates uncertainty or panic.
- can cause wasted time when activated.
- the virus could act as a hook for other malware

Problem 3 : R-4.5

- Virus
  - initial infection requires some sort of user assistance, such as clicking on an email attachment or sharing a USB drive.
  - can replicate itself by modifying other files or programs to insert code that is capable of further replication

- Worm
  - A computer worm is a malware program that spreads copies of itself without the need to inject itself in other programs, and usually without human interaction.
- Worms typically spread by exploiting vulnerabilities (e.g., buffer overflow) in applications run by Internet-connected computer systems that have a security hole. A worm then propagates by having each infected computer attempt to infect other target machines by connecting to them over the Internet.

- Trojan Horse

  - appears to perform some useful task, but which also does something with negative consequences (e.g., launches a keylogger)
  - Trojan horses can be installed as part of the payload of other malware but are often installed by a user or administrator, either deliberately or accidentally.
  - The main risk of a Trojan horse is that it allows an attacker to perform a task as if he were another user, possibly even a system administrator.

- Similarities: use up computing resources and can have great harmful affects on systems

**Problem 4 : R-4.13**

- privacy invasive software through Trojan horse method
- vulnerability: social engineering through "Baiting" (chapter 1)

- some said insider (okay but stretching it a bit)
- some said user is vulernability (okay)
- some said vulnerability is Autorun (okay)

**Problem 5 : R-4.15**

- would make it less likely that all the instances of the virus would be discovered.
- Don't have to indentify new vulnerabilities as soon
  - cheaper as far as development time goes
- This can be a selling point to purchasers of the malware
  - "Even if the signatures of other purchasers of this product are discovered, your signature will not have been identified."

**Problem 6 : R-4.16**

- The software's claim is bogus.
- It is impossible to detect all malware.
  - halting argument proven by contradiction
- New viruses can occur over time. Heuristics to detect new viruses are never perfect. There are always unknown vulnerabilities (zero-day attacks)
  - not recognizable by simple signature-based schemes
- Big risk of overwhelming number of false positives
- what about worms and Trojan hourses?
Problem 7 : C-4.4

- We need to figure out, given that QSniffer reports a found virus (F = Found), the probability that this is really the case (I = Infected).

- You don't have to understand all this (look at the description afterwards)

Probability of F given I = P(F | I) = .95  
Probability of not F given I = P(not F | I) = .05  
Probability of not F given not I = P(not F | not I) = .95  
Probability of F given not I = P(F | not I)= .05

Bayes Theorem from probability

\[
\text{Probability (Infected | Found)} = \frac{P(I | F) \cdot P(I)}{P(I | F) \cdot P(I) + P(F | not I) \cdot P(not I)}
\]

\[
= \frac{.95 \cdot .01}{.95 \cdot .01 + .05 \cdot .99} = .16 \text{ or } 16\%
\]

- Verbal explanation:

- because there are so many more uninfected PCs than there are infected ones, it is more likely that a positive report (a virus was detected) came from an uninfected PC (false positive) and than an infected one (true positive).

- so given a found report it is more likely (84%) that the computer is uninfected than is likely (16%) that it is infected.

-1 wrong numerical answer but in the neighborhood  
-2 majorly wrong numerical answer  
-2 no numerical answer given  
-2 no math work shown  
-1 wrong verbal explanation but has some sense  
-2 totally wrong verbal explanation  
-3 no verbal explanation

Problem 8 : C-4.8

Because this particular keylogger may not be distinguish which apps the keystrokes are from, you could mix up the keyboard character entries for the web browser and the text editor by switching randomly between them (using mouse click) during entry of the web browser user ID and password.
Another possibility, is to enter the alphabet into the text editor and copy and paste the user ID and password into the web browser fields.