# ISEC 400 Homework 12

Answer the following questions based on your reading of the text book, any supplemental material, and the instructor’s presentation this week. If you use an external source (i.e. a web-page, the required textbook, or an additional book) to help you answer the questions then be sure to cite that source. Hint: you should probably always be citing a source.

## Questions

1. [4 points] What is a “propagation vector,” for malware? List and describe four common propagation vectors for malware.
2. [4 points] Explain how a common Internet worm (such as Code Red, Nimda, or SQL Slammer) propagates so quickly. What can businesses do to prevent such worms from (a) infecting their computers and (b) allowing their infected computers from infecting others.
3. [4 points] Describe, in your own words, how a buffer overflow occurs and how it is exploited. What steps should developers take to prevent exploitable buffer overflow flaws from being written into their software?
4. [8 points] Watch the video “[Overflow Exploitation, Step By Step](http://www.youtube.com/watch?v=8xonDJe3YxI)” from David Hoelzer. Summarize and critique Hoelzer’s presentation (good, bad, and ugly). Pay particular attention to the processes of analysis, fuzzing, and developing the exploit. What did you find interesting, confusing, or surprising?

## Submission instructions

Create a Word document with your solution to the short answer questions. Submit the Word document to the dropbox for the course.