Review

- Summarize what you learned from the s1.0 and s1.1 lectures

Activity 1

Skim through this article and see if you can answer the following questions: (Look in the results and analysis section)

- Where do most security incidents occur?
- By whom are they perpetrated? What countries?
- What are the different categories that these incidents are frequently grouped into?
- Any other things that jump out to you or you find interesting.

Be prepared to present your findings.

Activity 2

Let us do some simple reconnaissance. Find some different web tools that will gather information for you about the cit.cs.dixie.edu website. We are not trying to hack anything at the moment, just gathering information.

Answer the following:

- what information did you find?
- What could you do with this information?
- Is there any way to prevent this information from getting out?
- Can you figure out what version of Apache is running? How about what ports are open? What OS version is it running?

(Hint: start by doing a Google search for online reconnaissance tools)

Activity 3

Find 3 current vulnerabilities for a program of your choice (wordpress has some if you can’t think of other programs):

- http://osvdb.org/
- http://www.us-cert.gov/ncas/current-activity/
- http://secunia.com/community/advisories/search/

Answer the following:

- Why do vulnerabilities exist?
- What information is provided about the vulnerability?
- How is it suggested to be fixed?
- Other relevant info?

Conclusion
Exim example