1. ~~I would like more info on system hardening in ch 3.~~
2. ~~What are Buffer overflow Input Attacks and what are Integer overflow Input Attacks?~~
3. ~~What are some ways that a user can investigate whether a keylogger has been installed on their system?~~
4. Why do browsers not block web beacons? Are they hard to detect/'blend in'? Are web beacons common/on most websites?
5. **A famous Buffer Overflow attack is the “Ping of Death” ; the book mentions that its size was 65,535 bytes. This number doesn’t strike me as particularly large, is there some reason that machines have trouble processing large pings or is this something that is no longer a threat today due to increased processing capabilities?**

I believe the issue lies not in the processing power available to computers but the maximum size allowed for a packet by TCP.

The maximum packet length per the TCP specification is 65,535 bytes, with most packets being far smaller than this. Because this is the specification, a receiving machine may only allocate a memory buffer up to this size, but someone with malicious intent can send a fragmented packet where each fragment is at or below the MTU(maximum transmission unit) set by the data link layer. When this happens the fragments make it through the data link layer and are reassembled by the receiving machine into a packet that is larger than 65,535 bytes and could possibly cause a buffer overflow which makes the machine malfunction or crash.

1. How is threat risk modelling accomplished? if it is performed before the code is written, how can an automated tool find security risks from specifications alone?
2. ~~How do rootkits persist across installs? Do they hide themselves in the mbr(master boot record)?~~
3. What programming languages currently in use today are considered “safe”?
4. In the section on thin client web applications, the textbook states that web applications provide several advances over client-server applications.  One is "thinner clients" (pg. 94). What do they mean by "thinner clients"?
5. Do web beacons have any other uses other than what we have learned about them so far?
6. ~~the longer the password, the harder it is to crack and the longer it takes, is there any other characters needed?~~
7. What are some ways to help protect and prevent with tampering of code in a SDLC?
8. I don't quite understand the difference between the various buffer overflow attacks we studied this week (Stack buffer overflow, NOP sled attack, Heap overflow, Jump to register attack).  If someone could help clarify the the differences between these, that would be great!
9. What are emanations and how do they get picked up by attackers?
10. What is the most effective way to counter malwares? or good countermeasures that help with preventing malwares and other attacks?
11. ~~What's the differences between anti-spyware and anti-malware, since spyware is a type of malware?~~
12. ~~How is cross-site scripting different from SQL injection?~~
13. If pharming is done to redirect consumers from one commerce site to another (that has an obvious different web design and name) as an unethical approach to compete with your rivals; is it illegal to do so if there is no malicious intent to the consumer?