1. I would like to know more about DoS and DDoS attacks.  What software or code do attackers use and what goes into writing the code before they use it on a victim?  Is this usually done using software that is preset or is it like in the movies - where an attacker seems to hop on any old computer and launch the attack in like 1 minute of keyboard strokes?
2. What are examples of situations where Kerberos mutual authentication would be appropriate/recommended?
3. (2 similar questions) What is the difference of an internal and an external audit? When would one be used over the other? Does the audit change depending on if its internal or external?
4. (2 similar questions):  Rainbow Tables seem to provide a really effective way to crack passwords, while it seems to take up a lot of space that doesn’t seem like much of a problem when you can get a portable hard drive with terabytes of storage. How would you defend against this? The book mentions “salting” hashes but what does that entail?

Rainbow tables work by comparing a password hash to a massive table of previously reversed password hashes. The most effective ways to avoid having a password that can be cracked using a rainbow table are to use long complex passwords and to salt.

Ideally, using a long and complex password that is hashed using a strong algorithm like AES-256 or AES-512 will result in a hash that is impractical to reverse, and therefore would not appear in a rainbow table of previously reversed password hashes.

Salting involves adding random bits to the input value of a password before it is hashed. This ensures that the resulting hash of the password is unique. The difference between this and an unsalted hash is that an unsalted hash will always be the same if the input for the password is the same, where salted input will produce unique hashes even in the case where the input is identical, thus rendering rainbow tables ineffective in reversing it.

1. ~~I'm having a hard time understanding and remembering the difference between Identification and Authentication due to how similar they are. Is Authentication just a more strict or thorough form of Identification, or is there differences between the two that need to be remembered?~~
2. ~~(2 similar questions) I'm still not sure the difference between a DoS attack and a DDoS attack. I know it basically the same thing, but is there anything different between them?~~
3. What are some common ways that an attacker might bypass biometric authentication? What is considered to be the most foolproof implementation of biometric authentication?
4. ~~what does the term false reject rate refer to?~~
5. ~~How would you help train employees to stop forms of social engineered attempts to gain access to the building?~~
6. How can I avoid SQL injection for website written by html and php?
7. I was hoping someone could provide a bit more clarity on the difference between deterrent controls and preventive controls.  For example, the book lists fencing as a preventive control, but lists razor wire as a deterrent control.  In my mind, these would belong to the same category.
8. ~~Why are buffer overflows so common when the fix of limiting user input is so easy?~~
9. ~~What is the best biometric authentication security measure?~~
10. ~~What is the main difference between spoofing and masquerading?~~
11. If "salting" a hash can stop Rainbow tables attack, why aren't we adding "salt" to all the hashes? Does it take up valuable resources?
12. Would implementing separation of duties to the administration of access control be beneficial in an organization?