COMP 5370/6370

Last Exercise/HW-Z (This will be a warm up for studying for the final too)
Please turn in via Canvas by 1:59pm on Friday, December 4, 2015.

Open book, notes, Internet, closed neighbors and friends and classmates. Answer with a definition, explanation, references to the web.

1. If you are given all the resources to setup a home network. Explain the steps you would take to secure the home network. Intrusion detection? How about bot detection (is a computer in my home network a bot?)?

2. Recapitulate the principles of classical and modern crypto; differences between symmetric and asymmetric. Why people do people use both?

3. What is XSS? Why does it matter? How to prevent?

4. What are usual ways to authenticate a person into a system.

5. What are the measures you would take for securing on the fly data and resting data?

6. Explain how a network intrusion detection system works.

7. Explain the differences between authorization and authentication. Given a brief explanation each of LDAP, DNS, Kerberos and Active Directory.

These are "improved" (you may decide "improvised") and expanded versions from

http://resources.infosecinstitute.com/top-50-information-security-interview-questions/

You can find some of the answers there. But don't just copy down what you see there please. ☺

Read through all questions from the last one in "Level 1," then "Level 2: The Break/fixer" and up. Level 1 questions are mainly about "how to interview."

8. Read up and study "TOR," the "deep web," and document its major features, threats, its evolution, and key implications for security (150-200 words, references, definitions, etc). How is the deep web different from an IntraNet in a company. What if a series of companies shared a private web site… how would it be like and unlike the deep web (besides the criminality issue).

Grad Students only:

9. Please explain Spear Phishing, Phishing, DNS cache poisoning, and keylogging. How do they work together?