CPTR 427 Midterm Exam Review

You should be familiar with the following figures from the Textbook: Figure 1.2, 7.9 and Table 2.3.

1. Be able to Describe ITU-T X.800. See Chapter 1 of Stallings Network Security. What 3 major categories are there and how do they relate? Make sure you can list some examples of each category.
2. Definitions for the following need to be understood: (sorry but I’m not doing this work for you. You can find definitions for these in your book or online. Remember that I did give you a def. for Hacking vs. Cracking).

|  |  |
| --- | --- |
|  | Authentication |
|  | Authorization |
|  | Computational Security |
|  | Cryptanalysis |
|  | Cryptography |
|  | Cryptology |
|  | Data Confidentiality |
|  | Data Integrity |
|  | Non-repudiation |
|  | Unconditional Security |
|  | Steganography |
|  | Hacking |
|  | Cracking |

1. Be able to calculate the number of keys for a cipher (e.g. if we have a 8 bit key, there are exactly 2^8 permutations and hence 2^8 keys.) Given that each key can be checked in .5 seconds, how long would a brute force attack take? Also be able to do this for a substitution cipher.
2. Be able to describe the different substitutions ciphers we talked about (particularly Vigenere) and how one would go about a successful attack.
3. ***What two concepts did Claude Shannon introduce that are used in ALL modern symmetric ciphers and are the basis for their cryptanalytic difficulty? (Describe each concept in detail! How do they relate to the use of the key/data?)***

Confusion and diffusion. Make sure you know them!

1. What basic operations are performed in the DES cipher algorithm? How many rounds are there in the algorithm? In fact I should be able to ask you anything about DES at this point.
2. Permutation, Circular Shift, XOR, SBox, SWAP
3. 16 rounds
4. …
5. What characteristics are needed for a good random number generator?

Every number should be just as likely to occur as any other number in the set AND the sequence should not repeat for a very long time. In addition, no sub-sequence of the series should be predictable.

1. List the OSI network layers from top to bottom. You know them…
2. Be able to list and describe the tools we have used in the small number of labs we’ve done so far.

We’ve used: iptables, nmap, webscarab, webgoat,

1. What OS is the most secure? Explain. (THIS IS NOT AN OPINION QUESTION)

Any modern OS can be as secure as any other modern OS (within reason), it all depends on the administrator configuring it.

1. Describe two approaches for designing a firewall policy. Which should be used and which should NOT be used?

DEFAULT: DENY ALL, poke holes for services you run.  
DEFAULT: ACCEPT ALL, Deny services we don’t want people to have access to.   
Of course the first one is the correct one.

1. What is TCP finger printing?

Using the implementation of TCP (they are not all the same) to determine the OS running on a system.

1. Describe hacking vs cracking.

Hacking is the use of a system of purposes other than what they were intended with or without permission. Hacking is generally associated with manipulating a system to learn more about how it operates and often misusing it. Cracking is the act of hacking without permission and with the intent to do damage illegally. Cracking is never legal, don’t believe me? See my definition.

1. (5) What did a deciphered document of Louis IV reveal about the identity of “The Man in the Iron Mask”

The man in the iron mask was a disgraced general that was imprisoned for cowardice.

1. All Lab questions are up for grabs on the exam.

See the answers on line.