Activity 2.2

1. Why 28 bits for “Tr0ub4dor&3”?
This is because the password follows a simple pattern of a dictionary word + a couple extra numbers or symbols, hence the entropy calculation is more appropriately expressed with log2(65000*94*94), with 65000 representing a rough estimate of all dictionary words people are likely to choose.

2. Why 3 days for guessing “Tr0ub4dor&3”?
Since there are 86400 sec’s in a day, that mean there are 1000 guesses* 86400= 86.4 million passwords can be cracked, we know that there are 28 bits, if we divide 2^28/ 86.4 million, that will give us around 3 days to crack.

3. Why 44 bits for “correcthorsebatterystaple”?
It has 44 bits of entropy because four words randomly chosen from a list of 2048 words is 4 * log2(2048) = 44 bits of entropy.

4. Why 550 years for guessing “correcthorsebatterystaple”?
Four words and each word has 11 bits of entropy, and the entire word is ~52 bits of entropy, which gives us 2^44 = 550 years at a rate of 1000 guesses/sec.

5. What does the following statement mean: “A truly random string of length 11 (not like “Tr0ub4dor&3”, but more like “J4l/tyJ&Acy”) has log_2(94^11) = 72.1 bits?
With 94 being the total number of letters, numbers, and symbols one can choose. However the comic shows that "Tr0ub4dor&3" has only 28 bits of entropy. This is because the password follows a simple pattern of a dictionary word + a couple extra numbers or symbols, hence the entropy calculation is more appropriately expressed with log2(65000*94*94), with 65000 representing a rough estimate of all dictionary words people are likely to choose.

6. Why does the table claim that the entropy for the password “correcthorsebatterystaple” is 0?
“Thanks to this comic, this is now one of the first passwords a hacker will try. The only entropy left is a boolean statement: "Is this password correcthorsebatterystaple, yes or no?". The Author claims that because of the popularity of XKCD among the Computer Science community the password “correcthorsebatterystaple” is no longer an effective 44 bit password

7. What is the main lesson the comic is trying to teach?
The Main lesson the Comic is trying to teach the reader is the difference between a password that is harder for a password attack to succeed, based on the entropy and number of characters the password has, and a password with a lower amount of bits of

entropy. To the reader's surprise, the password that's harder to remember actually has a lower entropy and therefore is easier for password cracking software, or other password attacks to succeed.