h_3

CONNOR TAFFE

1. R-4.2

The existance of user `12345` is a backdoor. The user was used by the logic bomb to login and gain permissions to run `fix.exe` and `purge` which deleted the files on Omega's manufacturing server.

2. R-4.13

Eve uses a trojan horse attack, disguising her spywaere as a normal USB driver. She uses a "social engineering" vector, placing a usb with a logo supposed to fool the finder into opening the usb on, she hopes, a company laptop.

3. C-4.4

The probability a computer is correctly diagnosed is ninety five percent. If it has been diagnosed as infected, the probability is as follows:

$$\frac{0.01 * 0.95}{(0.5 * 0.99) + (0.01 * 0.95)} = 0.01883052527254708 \tag{1}$$

4. R-5.4

The sequence number for the `ACK` is 156955004, and the acknowledge number is 883790340.

5. R-5.5

No, the address indicates the location of a resource. If two interfaces have the same address, routing will fail to function correctly and each will fial to function properly.

6. C-5.4

Encrypt a message with the shared key k and then with the server's known public key k_p. If it is the real server, and we are actually sharing k with it, it should be able to send us back the unencrypted message encrypted with it's private key k_s to further ensure identity. We unencrypt the message with k_p and verify it is the same as what we sent. If so, we have verified that this is both the server we want and that it knows about k.

7. C-5.7

The attacker can guess the next random number the client will produce and thusly intercept the TCP handshake.

8. C-5.15

The latency from Chicago to Copenhagen is much longer than 10ms.

9. R-6.2

$0.99 * 65536 = 64880.64$ requests per second.

10. C-6.12

2^{16} tcp connections for sequential vs $2^{16} * ln(2^{16})$ connections for a random scan because it may choose a port it has already hit each random attempt. The real question is: why would you ever do a random port scan that didn't remove ports you'd already hit?