Homework Assignment 3

1. (10 points) Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?
2. (20 points) A program is written to compute the sum of the integers from 1 to 10. The programmer, well trained in reusability and maintainability, writes the program so that it computes the sum of the numbers from k to n. However, a team of security specialists scrutinizes the code. The team certifies that this program properly sets k to 1 and n to 10; therefore, the program is certified as being properly restricted in that it always operates on precisely the range 1 to 10. List different ways that this program can be sabotaged so that during execution it computes a different sum, for example, 3 to 20.
3. (10 points) One way to limit the effect of an untrusted program is confinement: controlling what processes have access to the untrusted program and what access the program has to other processes and data. Explain how confinement would apply to the earlier example of the program that computes the sum of the integers 1 to 10.
4. (10 points) Identify the problem in the code, and explain what issues it may cause.

int buf[1024];

int \*b=buf;

while (havedata() && b < buf + sizeof(buf))

{

    \*b++=parseint(getdata());

      }

1. (20 points) Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your email client, web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occurred? If you do identify malware on your PC, how can you restore it to safe operation?
2. (10 points) Suppose that while trying to access a collection of short videos on some website, you see a pop-up window stating that you need to install this custom code in order to view the videos. What threat might this pose to your computer system if you approve this installation request?
3. (20 points) Your boss hands you a computer program and its technical reference manual. You are asked to check for undocumented features of the program. How is this activity similar to the task of the previous exercises? How does it differ? Which is the most feasible? Why?