Introduction to Computer Security, exercise 3, 7.-11. 2. 2011

1. Introduce the malware Rootkit. What malware class does it belong to or does it form its own class? How is it detected and how can it be removed?

2. Make a summary of the SANS Institute page Security Predictions.

3. Read the SANS Institute list ”Top 25 Software Errrors”, especially the sublist ”Insecure Interaction Between Components”. For every error in the sublist, analyse if it can be avoided following some of the implementation rules.

4. One program used setuid-to-root privileges when performing some operations. Someone observed that it could equally well implemented as a server, in which case the program would authenticate the user, connect to the server, send the command and role, and then let the server execute the command.

   a) What are the advantages of using the server approach rather than the single program approach?

   b) If the server responds only to clients on the local machine, using interprocess communication mechanisms on the local system, which approach would you use? Why?

   c) If the server were listening for commands from the network, would that change your answer to part b). Why or why not?

   d) If the client sent the password to the server, and the server authenticated, would your answers to any of the three previous parts change? Why or why not?

5. The canary for StackGuard simply detects overflow that might change the return address. This exercise asks you to extend the notion of a canary to buffer overflow.

   a) Assume that the canary is placed directly after the array, and that after every array access canary is checked to see if it has changed. Would this detect a buffer overflow? If so, why do you think this is not suitable for use in practice? If not, describe an attack that could change a number beyond the buffer without affecting the canary.

   b) Now suppose that the canary was placed directly after the buffer but -like the canary for StackGuard- was only checked just before a function return. How effective do you think this method would be?