Name:

Information Assurance: Homework 7

Due November 12, 2010. No late handins, so we may post the answer key in time to help students study for exam 2.

1. Consider the recently posted tool, Firesheep http://codebutler.com/firesheep.
a. By using firesheep, are you attacking integrity, confidentiality, and/or availability? How?
b. Consider the ethical implications associated with developing and deploying such a tool. Use the ACM/IEEE software engineering Code of Ethics as you reference point. http://www.acm.org/about/se-code. Make an argument that the developer and deployer of Firesheep has been acting ethically or unethically.

2. The text describes Stealth viruses that use root kit techniques to hide information about files containing the virus.
a. Describe how a virus would use root kit function hooking techniques to hide its presence from anti-virus software.
b. What is one way the owner of the machine could detect the presence of such a stealth virus?

3. Consider a program posted at http://www.cs.illinois.edu/class/fa10/cs461/hw7.zip This simple program has not one but two buffer overflow vulnerabilities in two different functions. The program takes two arguments: -f1 or -f2 to indicate which function to invoke and a count of the number of bytes to allocate for a buffer.
    a. The zip file includes a Makefile which will create two binaries (tested on remlnx.ews.uiuc.edu). The hw8-plain binary is a vanilla gcc compile. Try this program on both version of the function with buffer sizes 100 and 200. What happens?
    b. The other binary creates hw8-protected which is the same program compiled with the stack-guard canary values (details of stack guard at http://www.usenix.org/publications/library/proceedings/sec98/full_papers/cowan/cowan.pdf). On the ews machines stack guard is not enabled by default, but this is not the case on all distributions. If you compile on some other machine, check your compiler's man page to determine whether you need to enable stack guard in this part or disable it in part a. Run the same experiments again. What happens this time?
    c. Libsafe uses a runtime approach to detect and protect against stack smashing. The man page is posted at http://www.cs.uiuc.edu/class/fa07/cs461/libsafe.8.html. Unfortunately, this library doesn't seem to work any more. Based on the man page, how do you think hw-plain would operate in the presence of libsafe?
    d. What is one unique benefit of each approach (stack guard and libsafe)?

Name:

4. Consider ARP cache poisoning.
    a. Describe how poisoning a computer's ARP cache enables you to launch a Man-in-the-middle attack on that computer.
    b. Suppose there is a tool that proposes to automatically protect a computer from ARP cache poisoning. It looks for rapid changes of mappings between MAC addresses and IP addresses. If it sees more than three different MAC addresses associated with an IP address within a configurable period of time (defaults to 30 seconds), it will block the IP address from the ARP cache until the system administrator can investigate. If you know a computer has this tool installed, how can you launch a denial of service attack on this computer?