

## Information Assurance: Homework 8

Due November 29, 2006.

1. Try one of two malware prevention/detection programs.
  - a. If you have administrative access on either a Windows or Linux system, you can try running a root kit revealer. You can get the Windows rootkit revealer from <http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.msp> You can get chkrootkit from yum on a linux system or you can download it from <http://www.chkrootkit.org/> Describe the results of running these tools on your system.
  - b. Otherwise, you can use LibSafe (<http://www.research.avayalabs.com/project/libsafe/> or <http://www.research.avayalabs.com/gcm/usa/en-us/initiatives/all/nsr.htm&Filter=ProjectTitle:Libsafe&Wrapper=LabsProjectDetails&View=LabsProjectDetails>) to detect a sprintf() buffer overflow error. If you do not have administrative access on the target machine, do not run “make install”. Instead set the LD\_PRELOAD environment variable to the location of the libsafe library, /home/shinrich/libsafe-2.0-16/src/libsafe.so.2.0.16, in my case. The man page for libsafe is posted at <http://www.cs.uiuc.edu/class/fa06/cs498sh/hw8/libsafe.8.html>. Show problem code snippet and report on results.
2. Consider how viruses might spread in computer systems that employ the following access control policies.
  - a. Uses Domain Type Enforcement such as employed in SE Linux.
    - i. Virus attached to file with a Normal\_User domain/type
    - ii. Virus attached to file with a Httpd domain/type
  - b. Uses Biba Integrity Policy
    - i. Virus attached to file at system low integrity label.
    - ii. Virus attached to file at system high integrity label.
3. Describe a set of constraints for the Clark-Wilson model that lead to a description of the conditions that an audit mechanism should detect, e.g., the action -> conditions as discussed in class and in the text. Give the conditions that should be logged to audit these constraints.
4. A network administrator at Motorola wants to contribute the netflow logs from his site to the Internet Storm Center for the greater good of global intrusion detection. Netflow logs contain the tuple information (source address, destination address, protocol, source port, and destination port) about network connections entering and leaving the site.
  - a. Pretend you are the boss of the network administrator. List 3 concerns you might have for releasing this raw data.

- b. For each concern, identify a means to anonymize the data. What, if any, information would be lost to the third party researchers at Internet Storm Center?