COSC 4397/6397 Security Analytics
Computer Science Department, University of Houston, Instructor: Rakesh Verma
Spring 2016, Reading and Practicals - 1, Due Feb. 9 at 4pm.

1. (Internet use is allowed/reading linux/unix manuals is OK) Select a machine on the University of Houston network outside of the Computer Science Department. For the machine you selected, use the nmap command to find out the open ports, and the services running on those ports along with their versions if possible. Turn in a detailed report with the IP address of the machine and your findings. Explain how you figured out that the machine is on the UH network but not in computer science. Explain the command to close a port on a Linux server in detail.

2. (Reading about firewalls/iptables is allowed) Investigate the firewall available on Linux/Unix called iptables. What is the command to block a range of IP addresses using iptables. Is iptables a stateless packet filter? Justify your answer.

3. (Internet is allowed for finding the system and its documentation) Find a free and reputable intrusion detection system available on the Internet, open source if possible. Explain in no more than a page, how it works. Also provide the name and URL of the system you found.

4. Is it possible to develop a program P that can analyze a piece of software to determine if it is a virus? Note that we are interested in exact methods, i.e., P should say yes only when the input program is a virus and no in all other cases.

5. What is the difference between statistical anomaly detection and rule-based intrusion detection?

6. How can an attacker take advantage of integer overflows and format string overflows? Construct realistic scenarios and explain carefully.

Academic Honesty Policy: No collaboration with anyone or anything in or outside the course is allowed on any homeworks, exams and programming assignments (yes, that excludes the internet as well) except if it is explicitly allowed on a problem. The appropriate help of the instructor is of course allowed and encouraged. Special Note for this assignment: Parts of this assignment specifically allow you to use the Internet/reading materials, but it is still prohibited for the parts that do not explicitly ask you to use it. You must list all your sources for every problem.