Online Safety Lab I

CS 102

Feb. 17, 2006

Name(s)

Introduction

This lab will help us discover:

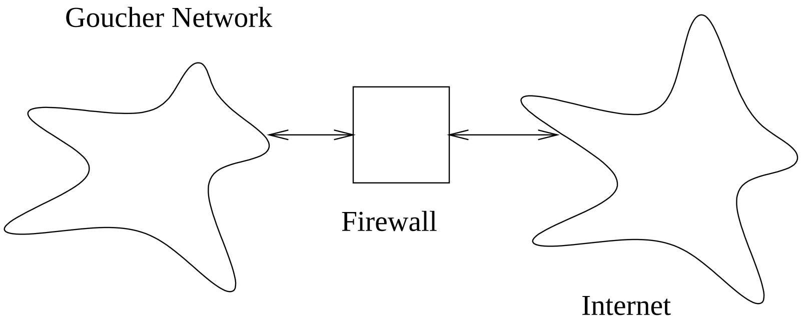
1. How effective our firewall protection is and what information our Web browsers are willing to reveal about us.
2. What limitations a software license agreement places over us.
3. How an online payment system works and how effectively it protects our privacy.

Lab

1. Visit Gibson Research at `http://grc.com/default.htm` and scroll down to ShieldsUP!. Click on the ShieldsUP! link, read through the page that appears, and click on the `Proceed` button. On the next page that appears, find the *ShieldsUP!! Services* and run both the "File Sharing" and the "Common Ports" tests. What firewall vulnerabilities did these tests reveal? Not all firewalls will protect against all possible attacks. This is a good test to run after installing or changing a personal firewall.

   Answer:

2. The relationship between the Goucher network, Goucher firewall, and the Internet looks like this:



The Gibson Research web site is on the Internet. Thus, it would have tested the Goucher firewall and any firewall installed on the PC from which you ran their two tests. With the relationship diagrammed, the Gibson tests could indicate that you're safe when you might actually still be vulnerable. Why might you still be vulnerable?

Answer:

3. Visit Privacy.net at `http://privacy.net/` and find the Network-Tools analyzer. Click this link. The site will show you how much information your computer is willing to reveal when you visit a Web page that asks for this information. Did it detect your Web browser and operating system correctly? Do you think a Web server needs to know these two pieces of information? Why or why not? Did it detect the color of your hair correctly? Which one of the findings on this page surprises you the most? (If you have time, click on the Cookie Demo link to learn what Internet cookies are and how they are used.)

   Answer:

4. A copy of the End User License Agreement for Microsoft Office is available at `http://phoenix.goucher.edu/~kelliher/cs102/eula.pdf`. (Refer to the HTML version of this lab on the class Web site for a link to this document — it will definitely save you some typing!)

   Are you allowed to install this software on more than one computer? Are you allowed to resell the software under any circumstances? Is there any part of the agreement that you disagree with strongly? Why? Have you ever read one of these agreements completely before today? What are some reasons you should read these agreements before installing the software they govern?

   Answer:

5. Visit PayPal at http://www.paypal.com/. How does it work? What do you need to set up an account? Is the sign-up page secure or not? What information does PayPal disclose to third parties? Where did you find the information disclosure answer?

   I often receive e-mail from PayPal that begins “Dear PayPal Member.” What is the name for this kind of a message, and is it legitimate?

   Answer:

6. Social engineering ploys rely upon our all-too-frequent natural tendency to trust others. Read this article:
   `http://en.wikipedia.org/wiki/Social_engineering_(computer_security)` and list an example or two of social engineering ploys below. Don't use the examples in the article! (Hint: Think of how a hacker could manipulate you if they gained control of a friend's e-mail account.)

   Answer: