ComSec for A+ Certification: Chapter 23

Summary
Students learn the various threats to both computers and data in this lesson. Basic security techniques will be explained in order to control the local environment. External threats to the network will be explored and discussed.

Engineering Connection
The IT technician is one of the first lines of defense versus a network threat. These threats can be both external as well as internal. Due to the fluid nature of network attacks in the 21st century, computer security is paramount. The lesson will have the student move through an internal network securing a single pc against known threats. The vocabulary will be given as homework, with the exercises demonstrating the myriad of vulnerabilities within a network. Stepping Stone Detection will demonstrate current exploits and vulnerabilities in today’s network.

Contents

I. Learning Objectives  
II. Introduction  
III. Background  
IV. Vocabulary  
V. Assessments  
VI. References  
VII. Other

Grade Level: 10-12  
Lesson #: 1 of 5  
Time Required: 120 minutes  
Lesson dependency: none  
Keywords: security, computer, software  
Reviews:

Related Curriculum:
Subject areas: Information Technology  
Curricular Units: Networks

Educational Standards: National Science Education Standards  
TEKS locations: 19 TAC Chapter 125 subchapter C: 46 Computer Technologies:  
4C: demonstrate knowledge of new and emerging technologies that may affect the field of computer technology.
Learning Objectives
After this lesson students will be able to:

1. Explain the various threats to both computers and data.
2. Use basic security techniques in order to control the local environment.
3. Identify external threats to the network.

Introduction
Some buffer overflows can work the same way as a virus. Buffer overflows were the security bug of the 1990’s – cross-site scripting and SQL injection soon took over as the high-profile threats this decade. But buffer overflows still wreak havoc on many systems because our network defenses don’t have the context in which to understand well-crafted buffer overflow attacks. Take for example a string of data that comes over the network pipe. It may be part of a picture, it may be text, we don’t know. But neither does the firewall watching the traffic. If this data happens to be part of a Flash, WMF, or PDF file, for example, the firewall has no way to determine if it is innocuous or evil. Firewalls have no context in which to understand how a piece of network traffic is going to be used by an application. In this example, an input buffer on a piece of freeware, e.g., Flash Player, Adobe Acrobat Reader, etc. can be overflowed and the client machine compromised very easily. Can’t happen you say? This exact vulnerability existed for years until early 2006 in a ubiquitous piece of web software… and no network defense in existence could stop it from being exploited.

The UTA-RET research on the next generation of network vulnerability in this arena will be reviewed and discussed.

Generate ideas: Using MM guidelines walk the students through the security features of Windows XP and Vista. When discussing bandwidth issues, use RET research data. Present the results and how the researching network attacks can help in both corporate and government security.

Lesson Background
Start with the 5 areas of a threat. Discuss the local network and data storage and movement. Explain social engineering and the need for interpersonal skills in combating threats. Stop to ensure understanding of the lesson by going over terms verbally around the room. Continue with examples of social engineering within your work experience. Initiate survey and discussion of corporate expectations and external threats. Lecture on the various aspects of security when using a local network. Have all students write definitions in engineering portfolio under Notes. When discussing bandwidth issues, RET research. Present the data and how the researching network attacks can help in both corporate and government security.

Vocabulary
Spam: unsolicited email.
pop-ups: unannounced browser windows that are sometimes difficult to close.
Malware: (malicious software): most often a Trojan.
Trojans: program that is labeled as one application but does something else.
Spyware: software that sends browsing information back to its originator.
Worms: similar to a Trojan except it travels from computer to computer.
Virus: a program that leeches onto a computer, attaching itself and then executing its program.
Adware: not usually harmful, sends display ads to browser, similar to Spyware.
Grayware: leeches bandwidth, popular programs like BitTorrent.
Firewall: designed to protect an internal network from unauthorized access both to and from the Internet.
Antivirus: a program to both actively and passively monitor and eliminate virus activity.
Encryption: enables unreadable data packets
Certificates: encrypts a browser window and verifies the company’s validity.
Authentication: proving who you are using a username and password.

**Exercise**
Demonstrate UAC on Vista and the improvements over XP. Use the classroom computers for XP and the lab computers for Vista.

**Assessment**
- Pre: 5 question quiz on whiteboard at beginning of class.
- Homework: notebook check
- Post: Chapter 23 Quiz, MM All-In-One 6th Ed.

**References**
- Mike Meyers *A+ All-In-One Certification 6th Ed.; Security Innovation whitepaper Biggest Information Security Mistakes that Organizations Make and How to Avoid Making Them; Dept of Computer Science and Engineering UTA – Stepping Stone Detection under the cloak of MMS*

**Other**
By setting at the outset of my class, a written standard of conduct within the classroom, I have established my environment as a workplace, instead of a traditional classroom. The students are expected to work in teams and various strategies within a TQM framework are utilized. When a topic hits home with 2 or more of my students in class, we discuss the subject in an open forum, which I moderate for control. This last occurred with the election of President Obama and it lasted for an entire hour. I felt that all of my students in that case needed to be heard for their opinions due to the historical significance. Workplace etiquette is continually reviewed, as I recommend students to local employers as well.