CRN: 72505 *Pace University* Fall 2009

IT662: Web and Internet Security

Instructor Dr. Lixin Tao, ltao@pace.edu, http://csis.pace.edu/~lixin
GC Office: GC416A, (914)422-4463
PLV Office: G320, (914)773-3449

Lectures 100% online through Pace Blackboard at http://blackboard.pace.edu

Office Hours Daily two hours online, Thursdays 2PM – 6PM upon appointment at office GC416A or G320 Goldstein Pleasantville. Please let me know your preferred meeting time and location so I could be there for you on time.

Description

Web and Internet security overview; limitations of firewall and IDS; HTTP and web technology overview; securing web servers, application servers, database servers, input validation, session management and Java EE servers; preventing URL hacking, cyber graffiti, e-shoplifting, session hijacking, impersonation, buffer overflows and virus and worm attacks.

Learning Objectives

After taking this course, a student should be able to

- Understand why firewall and IDS are not enough for securing e-commerce
- Understand the general structure, technologies and security weak spots of web computing
- Set up and secure Windows and Linux systems, Web servers and Web services, and database servers as well as sample e-commerce applications
- Use security tools including *nmap* and *netcat* to analyze and report on the security weaknesses of existing operating systems, web servers, database servers, and e-commerce applications
- Understand the impact of web security on the coming server-side computing technologies
- Conduct research in the related areas and apply the knowledge in securing specific IT environments

Textbooks

- ***Web Hacking: Attacks and Defense***, Stuart McClaure, Saumil, and Shreeraj Shah; Addison-Wesley 2003, ISBN 0-201-76176-9 [new editions are fine]
- ***Web Security for Network and System Administyrators***, David Mackey, Thomson Course Technology 2003, ISBM 0-619-06495-1 [new editions are fine]
- Class notes and course material posted in Pace Blackboard

Course Projects

You will be assigned into teams of around 10 people each. Each team will elect its team leader who will be responsible for coordinating the project activities and communicating with the instructor. In October the instructor will post potential course projects and each team can make suggestions too. Typically each team will install and configure some web servers, database servers or web security tools on a virtual *Windows Server 2003 Enterprise* PC or on a virtual *Ubuntu* Linux PC. At the end of the semester, each team needs to submit a comprehensive report on its project.

Course Virtual VMs

For your convenience, the instructor will distribute image files of VMware Virtual Machines (VMs) with *Windows Server 2003 Enterprise* and *Ubuntu 9.04* pre-installed and post them at http://csis.pace.edu/~lixin/download/WindowsServer2003Enterprise.exe, and http://csis.pace.edu/~lixin/download/ubuntu904.exe. You save the two downloaded files in the same folder "C:\VM" of your hard disk, and double-click on each of them to run them to completion (each taking a few minutes). This process will create two folders "WindowsServer2003Enterprise" and "ubuntu904". You can download the free *VMware Player* at http://csis.pace.edu/~lixin/download/VMware-player-2.5.1.exe to run the virtual VMs as normal applications on your Windows XP or Vista PCs. To install VMware Player, just run the downloaded file. You will find information on how to run the virtual VMs in the "readme.txt" files of the unzipped VM folders. To run either of the two VMs, just double-click on the file with icon of three overlapped blue squares in the corresponding folders. Acknowledge "I moved it" if asked. To get the logon window for Windows, use Ctr+Alt+Insert instead of Ctr+Alt+Delete. Please keep a fresh copy of the downloaded VM image files for recovering to their initial states whenever necessary. To run the VMs, your PC needs at least one GB memory and at least ten GB free disk space. If you don't have such a PC, you can also copy the VM folders "WindowsServer2003Enterprise" and "ubuntu904" on a portable disk and run them at one of the Pace lab PCs that has VMware Player installed (or you can install it on the spot). You can watch my video tutorial at http://csis.pace.edu/~lixin/vm to learn how to set up and run my VMs, even though your VMs are different. The free *VMware Player* doesn't work on Macs. If you need to run the VMs on a Mac, you need to buy a license of *VMware Fusion* (http://www.vmware.com/products/fusion/) for about $80, and VMware Fusion can also let your Mac run both Mac OS and Windows.

Bi-Weekly Course Assignments

Every two weeks, read post *What to Do Weeks X and (X+1)* (normally the first post) under **Discussion Board|WeeksXand(X+1)** (X will be replaced by a number) to see which tasks you need to finish for the two weeks. The bi-weekly assignments will cover reading assignments, discussion questions and (individual) project assignments. The bi-weekly course assignments will be posted on the Sunday of the first week of the period. Unless otherwise specified, all the tasks specified in a course assignment must be completed within the same two-week period and submitted by the Sunday at the end of the two-week period. A one-hour open-book online quiz will be conducted from 8AM Friday morning to 11PM Sunday evening of the second week of each period, through the Pace Blackboard, to check your understanding of the fundamental concepts and practices covered by the assignments for the two-week period.

Assignments Submission

The submission deadline will be strictly enforced. Each working day after the submission deadline would incur a 10% penalty on the assignment's grade. All files for a period's assignments should be zipped into a single file and submitted by attaching the solution zip file in a public reply message to the proper assignment thread in the **Discussion Board**.

Participating in Course Discussions

Every two weeks the instructor may post one or more questions in **Pace Blackboard Discussion Board** (**Discussion Board|WeeksXand(X+1)**). Students will conduct discussion on the posted questions by replying to the questions in the **Discussion Board** within two weeks from the posting of the questions. You can also comment on other student's responses. You can get credit by asking questions or helping to answer questions. A grade will be assigned in each two-week period to each student based on the

student's number and quality of participation in the **Discussion Board**. All postings must be formal with proper syntax and style, with citations to textbook pages or class notes to back up the arguments.

Grading Scheme

Course Project	30%	
Bi-week Assignments	30%	(Item Ds (discussion) in Blackboard grade records)
Quizzes	40%	

Comments

You are encouraged to send the instructor any comments or suggestions for the course. If you prefer, you can also post anonymous complaints in the *Water Cooler* of the Discussion Board. For immediate attention by the instructor, please send email to ltao@pace.edu.

CSIS School Policy Regarding Academic Integrity

1. Definition.

   Students must accept the responsibility to be honest and to respect ethical standards in meeting their academic requirements. Integrity in the academic life requires that students demonstrate intellectual and academic achievement independent of all assistance except that authorized by the instructor. The following constitute academic dishonesty. The list is not inclusive.

   a) Exams
      i) Copying from another student's exam.
      ii) Deliberately allowing other students to see and copy from your exam.
      iii) Using notes or calculators without permission from the professor or proctor.
      iv) Passing notes or calculators to other students without permission.

   b) Papers and projects
      i) Copying others' writing without proper reference.
      ii) Copying code or work from other students outside a team environment. This could be either from printouts and notes or from electronic media. This includes copying the structure of a program while changing cosmetic details such as identifiers and comments.
      iii) Deliberately allowing other students to copy your code or work, again either from printouts, notes or from electronic media. (This does not preclude a student "helping" another on a project as long as it is limited to giving information/hints and not code/solutions.)
      iv) Submitting a paper, program, or project that was done by someone else.
      v) Collaboration with one or more other students without the prior permission of the instructor.

2. Consequences. The following consequences will be affected:

   a) The first student offense may result, at the discretion of the instructor, in penalties including a zero on the offending course work or an F for the offending course.
   b) The second student offense in any course may result in an F for the offending course.
   c) The third student offense in any course may result in dismissal from the University.
   c) The Dean's office shall keep a student record of all student offenses occurring in courses offered by the School of CSIS including the first offense. This record should be destroyed when the student graduates from the University. The record shall be associated with the student and not with any particular course.

3. Procedures for determining an offense. The following procedure will be used:

   a) If the student admits to the offense, the appropriate penalty shall be enforced.
   b) If the student contests the charge, the Chair of the department in which the course was offered will make a decision as to the facts of the case. If the professor is also the Chair, this step could be skipped.
   c) If the student disagrees with the Chair's decision, he or she may request a hearing from the *Undergraduate* or *Graduate Scholastic Standing Committee*, depending upon the student's status. The Committee shall make a recommendation to the Dean concerning the facts of the case.
   d) Both the professor and the student may submit to the Committee relevant information in writing. The professor and/or the student may also appear before the committee, but usually not concurrently. No others may attend the Committee hearing, but the Committee may also consider the written statement of witnesses and other concerned persons.
   e) The decision of the Dean shall be final.
   f) A confirmed student offense shall be entered into the student's record in the Dean's office.