COSC 481
CASE STUDIES IN COMPUTER SECURITY
Course Description

Mike O'Leary
Office: 316K Stephens Hall
Office Phone: 410-704-4757
Email: moleary@towson.edu
Office Hours: MW 3:00 – 4:00

Spring 2005
MW 4:00-5:15
Room: YR 0401
Section: 101

Prerequisites: COSC 440 and COSC 450

Catalog Description: An in depth study of the practical aspects of computer security, including the study of common computer security vulnerabilities in a laboratory setting.

Course Objectives: To learn the practical, hands-on components of computer security.

Instructional Material. This course has no required text. Recommended readings will be discussed in class.

Methods of Instruction: The class will consist primarily of hands-on laboratory exercises in computer security. These will be supplemented by lectures and readings.

Academic Integrity: The nature of this course requires that students adhere to accepted standards of academic integrity. Violations of academic integrity include cheating, plagiarism, falsification and fabrication, complicity in academic dishonesty, personal misrepresentation and proxy, bribes, favors and threats. Cheating is a serious offense that will have grave consequences for your academic life.

Students who violate these standards will either fail the course outright or, at the instructor's discretion, may merely receive a zero on any assignment for which the student receives inappropriate assistance. Violations of these standards will be referred to the administration for possible additional action.

Students are reminded that they must follow the University Guidelines for Responsible Computing (http://wwwnew.towson.edu/adminfinance/ots/resp.comp.policy.asp).

Grading and Assignments: Each hands-on project will be graded; final grades will be determined by averaging the scores on the projects, after the lowest project grade has been dropped. The final project will count triple, and will not be dropped.

Attendance: Attendance is expected; you should only miss a class for a compelling reason. If you do miss a class, you are responsible for any material that you miss. It is quite likely that is will be impossible to make up a missed hands-on project.

University Policies: The last day to withdraw from the course with a grade of "W" is April 10. Students may not repeat a course more than once without prior permission of the Academic Standards Committee.

References:

Theoretical Books

- *Computer Security*, Matt Bishop, Addison Wesley, 2003.
- *The Practical Intrusion Detection Handbook*, Paul Proctor, Prentice Hall, 2001.
- *White Hat Security Arsenal*, Aviel D. Rubin, Addison Wesley, 2001.

Elementary Books

- *Counter Hack*, Ed Skoudis, Prentice Hall, 2002.
- *Hack Attacks Revealed*, John Chirillo, Wiley Computer Publishing 2001.
- *Hackers Beware*, Eric Cole, New Riders, 2002.
- *Hackers Challenge* , Mike Schiffman, McGraw Hill, 2001
- *Hackers Challenge 2*, Mike Schiffman, Bill Pennington, Adam O'Donnell, & Davi Pollino, McGraw Hill, 2003.
- *The Hacker's Handbook*, Susan Young & Dave Aitel, Auerbach, 2004.
- *Hacking Exposed*, Stuart McClure, Joel Scambray & George Kurtz, McGraw Hill, 2001.
- *Hacking Linux Exposed*, Brian Hatch & James Lee, McGraw Hill, 2003.
- *Hacking Windows 2000 Exposed*, Joel Scambray & Stuart McClure, McGraw Hill, 2001.
- *Hardening Linux*, James Turnbull, Apress, 2005.
- *Maximum Linux Security*, Anonymous, SAMS, 2001.
- *Maximum Security*, Anonymous, SAMS, 2001.
- *Network Security Hacks*, Andrew Lockhart, O'Reilly, 2004.
- *Practical Unix & Internet Security*, Simson Garfinkel, Gene Spafford & Alan Schwatrz, O'Reilly, 2003.
- *Web Hacking*, Stuart McClure, Saumil Shah, & Shreeraj Shah, Addison Wesley,
- *Web Security*, Lincoln Stein, Addison Wesley, 1998.

Firewalls & Intrusion Detection

- *Best Damn Firewall Book Period*, Robert Shimonski, Debra Littlejohn Shinder, Dr Thomas Shinder, Anne Carasik-Henmi, Syngress, 2003.
- *Defense and Detection Strategies Against Internet Worms*, Jose Nazario, Artech House, 2004.
- *Firewalls and Internet Security*, William R. Cheswick, Steven M. Bellovin & Aviel D. Rubin, Addison Wesley, 2003.
- *Hacker Web Exploitation Uncovered*, Marsel Nizamutdinov, A-List, 2005.
- *Incident Response*, Kevin Mandia & Chris Prosise, McGraw Hill, 2001.
- *Intrusion Signatures and Analysis*, Stephen Northcutt, Mark Cooper, Matt Fearnow, & Karen Fredrick, New Riders, 2001.
- *Managing Security with Snort and IDS Tools*, Kerry Cox & Christopher Gerg, O'Rielly, 2004.
- *Network Intrusion Detection*, Stephen Northcutt & Judy Novak, New Riders, 2003.
- *Network Perimeter Security*, Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Fredrick & Ronald W. Ritchey, New Riders, 2003.
- *Snort 2.1 Intrusion Detection*, Raven Alder *et. al*., Syngress, 2004.
- *Troubleshooting Linux Firewalls*, Michael Shinn & Scott Shinn, Addison-Wesley, 2005.

Programming & Security

- *Building Secure Software*, John Viega & Gary McGraw, Addison-Wesley, 2002.
- *Buffer Overflow Attacks*, James Foster *et. al.*, Syngress, 2005.

- *Essential PHP Security*, Chris Shiflett, O'Rielly, 2005.
- *Exploiting Software*, Greg Hoglund & Gary McGraw, Addison Wesley, 2004.
- *Hacking. The Art of Exploitation*, Jon Erickson, No Starch Press, 2003.
- *Hacker Disassembling Uncovered*, Kris Kaspersky, A-List, 2003.
- *Pro PHP Security*, Chris Snyder & Michael Soutwell, Apress, 2005.
- *The Shellcoder's Handbook*, Jack Koziol *et. al.*, Wiley, 2004.
- *Sockets, Shellcode, Porting & Coding*, James Foster & Mike Price, Syngress, 2005.

Networking and System Administration
- *TCP/IP Illustrated*, W Richard Stevens, Addison Wesley, 1994.
- *Upgrading and Repairing Networks*, Scott Mueller, Que, 2004

Other
- *Cyber Crime Investigators Field Guide*, Bruce Middleton, Auerbach Publications, 2002.