COSC 481
Case Studies in Computer Security

Class Policies

Dr. Mike O'Leary
Office: YR 307B,
School of Emerging Technologies
Office Phone: 410-704-4757
Email:moleary@towson.edu

Spring 2014
Class: TuTh 5:00 – 6:15
Room: YR 405
Section: 101
Office Hours: M 9–10, W: 10–11
& by appointment

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: Upon completing the course, students will be proficient with the core hands-on elements of computer security. In particular, students will be able to set up and securely manage common services, and will be able to manage common defensive measures including log servers, intrusion detection systems and firewalls.

Tentative Schedule:

- **1/28, 1/30**. Introduction to Kali Linux; common offensive tools including Nmap, Metasploit, and Armitage.
- **2/4, 2/6**. Setting up a BIND DNS infrastructure.
- **2/11, 2/13**. Domain controllers and Active Directory. Windows Server 2008 R2 and Windows Server 2012. Group policy. File Shares.
- **2/18, 2/20**. Logging in Windows and Linux. Splunk. NTP.
- **2/25, 2/27**. SSH, Situational awareness. Autopsy & forensics.
- **3/4, 3/6**. Live exercise.
- **3/11, 3/13**. Apache 2.2 on Linux. ModSecurity.
- **3/18, 3/20**. Spring break.
- **3/25, 3/27**. IIS.
- **4/1, 4/3**. Snort. Intrusion detection systems.
- **4/8, 4/10**. Live exercise
- **4/15, 4/17**. MySQL. Barnyard.
- **4/22, 4/24**. Web Applications. Snort Report.
- **4/29, 5/1**. Firewalls, IPFire, VPN.
- **5/6, 5/8**. Advanced web applications. Nessus.
- **5/13, 5/15**. Live exercise.

Course Material: Lecture material for this course will available online at `http://cyberoperations.wordpress.com`

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, including any homework assignments given in that class. Unexcused absences can result in a lower grade.

Students should not attend classes or other university events from the onset of flu-like symptoms until at least 24 hours after the fever subsides without the use of fever reducing medications. Such absences will be considered excused absences; however, students are responsible for the material covered during the period of their absence.

Grading: Students will be asked to demonstrate that they have completed each weekly lesson by completing (live) assignments in front of the instructor. Together, these assignments will be worth 20 points.

Students will also be evaluated on the basis of three hands-on exercises. The first will be worth 20 points, the second worth 25 points, and the third worth 30 points toward the final grade. These exercises will have a team component and an individual component; both will be explained in detail in class.

Students who visit the professor outside of class, either during office hours or otherwise will receive an additional 5 points toward their final grade.

Given a final point score p, final grades will be assigned based on the following scheme

- $80 \leqslant \mathrm{p}$: A
- $78 \leqslant \mathrm{p} < 80$: A-
- $77 \leqslant \mathrm{p} < 78$: B+
- $70 \leqslant \mathrm{p} < 77$: B
- $68 \leqslant \mathrm{p} < 70$: B-
- $67 \leqslant \mathrm{p} < 68$: C+
- $60 \leqslant \mathrm{p} < 67$: C
- $50 \leqslant \mathrm{p} < 60$: D
- $\mathrm{p} < 50$: F

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://www.towson.edu/adminfinance/ots/aboutots/otspolicies/responsible.asp`.

University Policies: Students are reminded that may not repeat a course more than once without prior permission of the Academic Standards Committee.

Final Exam: The final exam time for this class is Thursday, May 15 from 5:15 until 7:15. This time will be used for the in-class portion of the final project. The final project will be due at 5:15 on Tuesday, May 20, and may be submitted electronically.

Bibliography: There are a number of books that cover various components important to this course, listed below are what I consider to be a few of the better choices listed in roughly the order the topics they cover appear in the class.

- Nmap network scanning: The official Nmap project guide to network discovery and security scanning, by Gordon Lyon, Insecure.Com, LLC, 2008
- Metasploit: The Penetration Tester's Guide by David Kennedy, Jim O'Gorman, Devon Keanrs and Mati Aharoni, No Starch Press, 2011.
- Defense against the Black Arts: How Hackers Do What They Do and How to Protect against It, by Jesse Varsalone, Matthew Mcfadden, Michael Schearer, Sean Morrissey, and Ben Smith, CRC Press, 2011.
- DNS and BIND (5th Edition) by Cricket Liu and Paul Albitz, O'Reilly, 2006.
- Windows Server 2008 Security Resource Kit, Jesper Jihansson and Microsoft MVPs with the Microsoft Security Team, Microsoft Press, 2008.
- Microsoft Windows Security Resource Kit by Ben Smith, Brian Komar, and The Microsoft Security Team, Microsoft Press; 2nd edition 2005.
- Hardening Linux by James Turnbull, APress, 2005.
- Apache Security by Ivan Ristic, O'Reilly, 2005.
- Windows Forensic Analysis (2nd Edition), Harlan Carvey, Syngress, 2009.
- Internet Information Services (IIS) 7.0 Resource Kit, Mike Volodarsky *et. al.*, Microsoft Press, 2008.
- Firewalls and Internet Security by William Cheskwick, Steven Bellovin, and Aviel Rubin, Addison Wesley, 2003.