COSC 481
Case Studies in Computer Security

Class Policies

Dr. Mike O'Leary
Office: YR 317
Department of Mathematics
Office Phone: 410-704-4757
Email:moleary@towson.edu

Spring 2017
Class: MW 5:00 – 6:15
Room: YR 405
Section: 101
Office Hours: M 3–4, W 1–2& 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.

Course Materials: The required textbook is M. O'Leary, *Cyber Operations*, Apress, October 2015. This book was custom-written for this course.

Expectations: This class is intended to help students become cyber security professionals. Students are expected to act professionally at all times.

- Always ethical, all the time. Students in this class will learn techniques for both defensive and offensive cyber-security. Students will use this knowledge in an ethical manner.
- Preparation. Students are expected to be prepared for every class. This includes having read the assigned readings in advance and being ready for each exercise.
- Respect. Students are expected to treat each other with respect at all times. Live exercises are fun, and hacking into other students systems is fun and often leads to of excitement and enthusiasm. This excitement and enthusiasm will always be respectful.
- Openness and Opportunity. This course has an open-ended design. The best students take the time to move out of their comfort zone and and learn more about areas where they are weak. A student that has extensive experience in Linux at work, should take advantage of the opportunity to learn more about Windows.

Schedule: This is subject to change for a variety of reasons, including weather-related closings. When in doubt, ask in class!

- **Week 1** (1/30, 2/1). Introduction to Kali Linux; common offensive tools including Metasploit, and Armitage. Operational Awareness. Examining processes, network data, and packet captures for evidence of intrusion. Readings: Chapters 2, 3.
- **Week 2** (2/6, 2/8). BIND DNS infrastructure. Chapter 4.

- **Week 3** (2/13, 2/15). Domain controllers and Active Directory. Windows Server 2008 R2 and Windows Server 2012. Group policy. Chapter 6.
- **Week 4** (2/20, 2/22). Logging and Log Servers. Basic Network Services. Chapters 8 & 9.
- **Week 5** (2/27, 3/1). Live exercise.
- **Week 6** (3/6, 3/8). Apache on Linux. ModSecurity. Chapter 11.
- **Week 7** (3/13, 3/15). IIS. Chapter 12.
- **Week –** (3/20, 3/22). Spring break.
- **Week 8** (3/27, 3/29). Firewalls (1/2). Chapter 14.
- **Week 9** (4/3, 4/5). Live exercise
- **Week 10** (4/10, 4/12). Firewalls; network segmentation (2/2). Chapter 14.
- **Week 11** (4/17, 4/19). MySQL/MariaDB. Chapter 15.
- **Week 12** (4/24, 4/26). Intrusion detection systems; Snort & Barnyard 2. Chapter 16.
- **Week 13** (5/1, 5/3). Web Applications. Chapter 18.
- **Week 14** (5/8, 5/10). Practice / Oops it snowed.
- **Week 15** (5/15, 5/17). Live exercise.

Grading: Students will 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.

There are eleven course checkpoints (below). Each checkpoint completed on time is worth two points towards the final grade. Checkpoints completed up to one week late are worth one point towards the final grade. Checkpoints are completed or not; there is no partial credit.

Students who visit the professor outside of class prior to Spring break, either during office hours or otherwise will receive an additional 3 points toward their final grade.

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

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

Checkpoints:

- **Checkpoint 1; due 2/8**. Provide a functioning Windows system, a functioning Kali system, and show that an exploit has been run on the Windows system to gain a shell.
- **Checkpoint 2; due 2/13**. For the shell in Checkpoint 1, on the Windows system identify the PID of the running process and provide a packet capture showing the traffic between the Windows system and the Kali system.
- **Checkpoint 3; due 2/20**. Demonstrate a functioning BIND system.

- **Checkpoint 4; due 2/27**. Demonstrate a functioning Windows domain with a desktop system connected to the domain.
- **Checkpoint 5; due 3/1**. Demonstrate a functioning SSH server that uses public key authentication.
- **Checkpoint 6; due 3/15**. Demonstrate a functioning Apache server that uses ModSecurity to block requests that include the text "zzz" in the request.
- **Checkpoint 7; due 3/27**. Demonstrate a functioning IIS server that uses ModSecurity to block requests that include the text "zzz" in the request.
- **Checkpoint 8; due 4/19**. Demonstrate a functioning network based on IPFire that uses a DMZ and an internal network.
- **Checkpoint 9; due 4/26**. Demonstrate a functioning MySQL or MariaDB server.
- **Checkpoint 10; due 5/3**. Demonstrate a functioning intrusion detection system that logs alerts to a database.
- **Checkpoint 11; due 5/10**. Demonstrate a functioning web application.

Class Structure: There will be essentially no lectures. Students are expected to have completed the assigned readings prior to coming to class. On non-exercise weeks, class time will allow students to work on checkpoints or on the exercises.

Classroom Computers: Systems in YR 405 are numbered on the monitor; the account used to log on varies with the computer.

- Username: `case01` - `case31`
- Password: `Sea*tigers`
- Home Directory: `D:\csVM\case01 - 31`

Most work will be done using virtual machines (on VMWare). A number of default images are available on the classroom lab share `\\labshare`; these include

- CentOS 6.2 x64
- Mint 13 x64 (Cinnamon)
- Mint 13 x86 (KDE)
- Ubuntu 12.04 x86
- Windows 7 x86
- Windows 7 x64
- Windows 8 x86
- Windows 8 x64
- Windows Server 2008 R2
- Windows Server 2012
- Kali 2016.2 (Updated January 2017)

In each case the default account name is `zathras` and the default password is `password1!`.

These systems are already built, have VMWare tools running, and include a full suite of tools (Browser, Java, Flash, EMail, Wireshark). Students are not required to use only these virtual machines.

Classroom Networking: The computer network in YR 405 is not connected to the Internet.

- **10.0.0.0/24** = 10.0.0.1 - 10.0.0.253 (gateway 10.0.0.254) is assigned by DHCP to the physical workstations in the class.
- **10.0.1.0/24** = 10.0.1.1 - 10.0.1.253 (gateway 10.0.1.254) is assigned via DHCP to virtual machines that are set up in class.
- **10.0.x.0/24** = 10.0.x.1 - 10.0.x.253 (gateway 10.0.x.254) for $x = 2, 3, 4, 5$ are available for students to use when building systems for practice that are not intended for use in an exercise. Team 1 may use 10.0.2.0/24, Team 2 may use 10.0.3.0/24, Team 3 may use 10.0.4.0/24 and Team 4 may use 10.0.5.0/24.
- **10.0.6.0/24** = 10.0.6.1 - 10.0.6.253 (gateway 10.0.6.254) is used by the instructor. Exercise Control lives at 10.0.6.250, and will be described in more detail in the assignments for the live exercises.
- **10.x.0.0/16** = 10.x.1.1 - 10.x.253.253 (gateway 10.x.254.254) for $x = 1, 2, 3, 4$ is used by student teams during live exercises.

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. 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.

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 Wednesday, May 17 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 Monday, May 22, and may be submitted electronically.