ITMS 448 - Cyber Security Technologies
Fall 2019

Maurice Dawson

Syllabus

Professor: **Prof. Maurice Dawson, Ph.D., D.C.Sc., SMIEEE, CSSLP, CGEIT, C|CISO**
Address: Perlstein Hall 10 W 33rd St, Room 223, Chicago IL 60616
Telephone: 312.567.5246
Mobile: 571.317.1893
Fax: 312.567.5283
Email: mdawson2@iit.edu
Office(s): Main Campus - Perlstein Hall 10 W 33rd St, Room 221E, Chicago IL 60616
Office Hours: Main Campus: By Appointment & 11:00 pm -1:00 pm WR

Course Catalog Description: Prepares students for a role as a network security administrator and analyst. Topics include viruses, worms, other attack mechanisms, vulnerabilities and countermeasures, network security protocols, encryption, identity and authentication, scanning, firewalls, security tools, and organizations addressing security. A component of this course is a self-contained team project that, if the student wishes, can he extended into a full operational security system in a follow-course.

Prerequisites: None

Credit: 3-0-3 *(lecture courses)* Semester Hours

Lecture Days, Time & Place: Class 5:30 pm - 9:05 pm W Stuart Building 113, 10 W. 33rd Street on IIT's Main Campus, or online via IIT Online.

Course Outline:

1. Careers in Cyber Security, Security Trends, Information Security and Risk Management, Introduction to Linux
2. Access Control, Bash Scripting, Introduction to NIST SP 800 Series
3. Security Architecture and Design, DIACAP IA Controls, Virtualization
4. Physical and Environmental Security
5. Telecommunications and Network Security
6. Cryptography and Cryptographic Applications
7. Business Continuity and Disaster Recovery
8. Legal, Regulations, Compliance, and Investigations
9. Application Security
10. Operations Security
11. Special Topics: Cyber Terrorism, Destructive Coding Practices, Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signatures Intelligence (MASINT), Open Source Intelligence (OSINT), Offensive Security, Defensive Security, Certification and Accreditation (DIACAP, NIST SP 800 Series, Common Criteria, NSA Rainbow Series, Directive of Central Intelligence Directives), Reverse Engineering

Textbook: The textbook for this course is **mandatory.**
Required Texts:

1. Gordon, A. (Ed.). (2015). Official (ISC) 2 guide to the CISSP CBK. CRC Press.
2. Recommended (freely downloadable) books and journals:
3. Anderson, Ross (2007) Security Engineering, 2nd Edition, Wiley (Free and available online at: http://www.cl.cam.ac.uk/~rja14/book.html)
4. Mead, Nancy., Allen, Julia., Ardis, Mark., Hilburn, Thomas., Kornecki, Andrew., Linger, Richard., & McDonald, James. (2010). Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum (CMU/SEI-2010-TR-005). Retrieved May 20, 2014, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9415
5. Dawson, M., Eltayeb, M., & Omar, M. (2016). Security Solutions for Hyperconnectivity and the Internet of Things (pp. 1-305). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3
6. Dawson, M., Kisku, D. R., Gupta, P., Sing, J. K., & Li, W. (2016). Developing Next-Generation Countermeasures for Homeland Security Threat Prevention (pp. 1-394). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0703-1
7. NIST Special Publications (800 Series): View all publications at http://csrc.nist.gov/publications/PubsSPs.html
8. Common Criteria Certification (CC v3.1.Release 4): View guidance at https://www.commoncriteriaportal.org/cc/

9. A Practical Approach for Combating Social Engineering In Your Enterprise http://csrc.nist.gov/organizations/fissea/2008-conference/presentations/Wednesday/Wednesday-ALewis_SocialEngineeringinEnterprise.pdf
10. A Practical Approach for Combating Social Engineering In Your Enterprise http://csrc.nist.gov/organizations/fissea/2008conference/presentations/Wednesday/Wednesday-ALewis_SocialEngineeringinEnterprise.pdf
11. In class discussion on covert channels using a Rainbow Series document. See http://fas.org/irp/nsa/rainbow/tg030.htm
12. Open-Source Intelligence https://fas.org/irp/doddir/army/atp2-22-9.pdf
13. Open Source Intelligence (OSINT) 2oolKit On The Go http://www.phibetaiota.net/wp-content/uploads/2009/07/OSINT-2ool-Kit-OnThe-Go-Bag-O-Tradecraft.pdf
14. Additional read ttps://www.researchgate.net/publication/264673051_Open_Source_Software_to_Enhance_the_STEM_Learning_Environment
15. English, A., & Ford, C. A. (2004). The HIPAA privacy rule and adolescents: legal questions and clinical challenges. Perspectives on sexual and reproductive health, 36(2), 80-86.

Expectations of performance

I expect all students to prepare for, **attend**, and contribute to the classes on a regular basis. Students will lose up to 10% of the course grade for poor attendance (see Attendance section below). Another forum for you to demonstrate your learning is through assignments or quizzes, which together account for 25% of the course grade. We will also perform "hands-on" lab assignments to better appreciate InfoSec concepts. Given the importance of practical experience in InfoSec, lab assignments are worth 40%. Finally, we will learn and explore InfoSec through a group research project worth 35%. This course does not have exams. Thus, your grade will be calculated as follows:

Undergraduate Students

Course Component
Lab Assignments (Individual work) • *Learn The Command Line* • *World News Assignment* • *Navigating Linux Task* • *Shell Scripting & Bash Scripting Task* • *Networking & System Admin Individual SkillsTask* • *Physical Security Task* • *Data Set Submission*
Lab Assignments (Group Work) • *Networking Penetration Task* • *Software Code & Threat Analysis Presentation* • *Cryptography Task* • *Group Project*
Final Exam *VM Final Exam*
NOTE: Up to 10% **loss** in final score for poor attendance

Course Component
Lab Assignments (Individual work) • *Learn The Command Line* • *World News Assignment* • *Navigating Linux Task* • *Shell Scripting & Bash Scripting Task* • *Networking & System Admin Individual SkillsTask* • *Physical Security Task* • *Data Set Submission*
Lab Assignments (Group Work) • *Networking Penetration Task* • *Software Code & Threat Analysis Presentation* • *Cryptography Task* • *Group Project* • *Research Paper*
Final Exam *VM Final Exam*
NOTE: Up to 10% **loss** in final score for poor attendance

Course Notes: Copies of the course lecture notes in the form of a PDF of the PowerPoint presentation accompanying each lecture will be provided for each student on Blackboard. This should be useful if you must miss a class. You should be aware that note taking is encouraged and should help your understanding of the material.

Course Web Site: http://blackboard.iit.edu/

Blackboard: The course will make intensive use of Blackboard (http://blackboard.iit.edu/) for communications, assignment submissions, group project coordination, providing online resources and administering examinations. All remote students will view the course lectures online via Blackboard, and online readings will be found on Blackboard.

Attendance: If you are in a live section of the class and will not be able to attend class, please notify me via email or by text message to 847.920.8442 prior to class time. Live section students who miss a class should always watch the lecture online.

Writing Assignments: There will be three additional writing assignments for this class. Below is a brief overview of final assignments.
Research Paper - Graduate Students: A research paper addressing a topic in *whatever you specify*. The paper will be fifteen to twenty pages long and will meet standards expected of a paper submitted for journal publication. Instructions for submission of the paper will be included with the assignment on Blackboard. You must fully attribute all material directly quoted and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. *Failure to format your bibliography entries in APA style will result in an automatic reduction of one letter grade for this assignment.* No more than twenty-five percent of material included in any paper may be direct quotes. No more than thirty percent of the resources cited may be from online. Submission of the paper for actual publication is highly encouraged. A basic outline for your paper—which should be at least three pages in length—will be due **February 4th**. The paper will be due **April 15th**. More specific instructions for the outline and the paper will be provided on Blackboard.

Examinations: The final examination will consist of an in-class essay examination measuring course outcomes as discussed above. The examination will be open-book, open note, and open-Web.
Internet students may complete this exam online. *(See exam statement for other options)*

Academic Honesty:

Plagiarism: All work you submit in this course **must be your own**. You must fully attribute **all** material directly quoted in papers and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. Students have submitted plagiarized material the last six times I have taught this course and **I will not tolerate it**. If you submit plagiarized material you **WILL** receive a grade of **ZERO** for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. **There is no excuse for not understanding this policy** and if you do not understand it please let me know and I will be happy to discuss it with you until you do. *(Should include assignment or lab collaboration statement as necessary.)*

Grading: Grading criteria for ITMS 448-548 students will be as follows:

A	*Outstanding work reflecting substantial effort*	90-100%
B	*Excellent work reflecting good effort*	80-89.99%
C	*Satisfactory work meeting minimum expectations*	70-79.99%
D	*Substandard work not meeting expectations*	60-69.99%
E	*Unsatisfactory work*	0-59.99%

Grading criteria for ITMS 448-548 students will be as follows:

A	*Outstanding work reflecting substantial effort*	90-100%
B	*Adequate work fully meeting that expected of a graduate student*	80-89.99%
C	*Weak but marginally satisfactory work not fully meeting expectations*	65-79.99%
E	*Unsatisfactory work*	0-64.99%

The final grade for the class will be calculated as follows:

Assignments	**28%**
Labs	**30%**
Exams	**42%**

*****An additional 10% will be random quizzes that will count for participation

Other Class Resources: Online readings and other class resources may be found at on Blackboard.

Our Contract: This syllabus is my contract with you as to what I will deliver and what I expect from you. If I change the syllabus, I will issue a revised version of the syllabus; the latest version will always be available on Blackboard. Revisions to readings and assignments will be communicated via Blackboard.

Disabilities: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312.567.5744 or disabilities@iit.edu.