IIT 443 Fall 2018 Syllabus

Professor: **Kevin Vaccaro**
Address: Perlstein Hall 10 W 33rd St, Room 233, Chicago IL 60616
Telephone: 708-529-1563
Email: *vacckev*@iit.edu
Office(s): Rice Campus -
Mies Campus - Perlstein Hall 10 W 33rd St, Room 233
Office Hours: Mies Campus: Tuesday 6:00-6:30pm (In Classroom)
Other times by request

Course Catalog Description: This course addresses hands-on ethical hacking, penetration testing, and detection of malicious probes and their prevention. It provides students with in-depth theoretical and practical knowledge of the vulnerabilities of networks of computers including the networks themselves, operating systems, and important applications. Integrated with the lectures are laboratories focusing on the use of open source and freeware tools; students will learn in a closed environment to probe, penetrate, and hack other networks. It is recommended, but not required, that students also take ITMS 448 prior to or in parallel with this course. (2-2-3).

Prerequisites: None Credit**:** 3-0-3 *(lecture courses) or* 2-2-3 *(lab courses)* Semester Hours

Course Outcome: Each student will be able to explain the professional hacker's methodology for attacking a network and differentiate between different methods of attacks and countermeasures.

Lecture Days, Time & Place: Tuesday 6:25 p.m. - 9:05 p.m., *Mies Campus IT 14C5-1*

Schedule of Topics/Readings: ***You should do all readings prior to class.***

Session	Date	Topic	Reading
1	8-21	Goal Based Penetration Testing	Chapter 1
2	8-28	Kali / Using Linux /Basic Scripting	Chapter 1
3	9-4	Open Source Intelligence and Passive Reconnaissance	Chapter 2
4	9-11	Active Reconnaissance of External and Internal Networks	Chapter 3
5	9-18	Vulnerability Assessment	Chapter 4
6	9-25	Physical Security and Social Engineering	Chapter 5
7	10-2	Reconnaissance and Exploitation of Web-Based Applications	Chapter 7
8	10-9	No class	
9	10-16	Attacking Remote Access	Chapter 8
10	10-23	Client-Side-Exploitation	Chapter 9
11	10-30	Bypassing Security Controls	Chapter 10
12	11-6	Exploitation	Chapter 11
		Initial draft of reports due for both Undergraduate and Graduate students (11-6)	
13	11-13	Action on Objective	Chapter 12
14	11-20	Privilege Escalation	Chapter 13
15	11-27	Command and Control	Chapter 14
		Final reports due December 6th	
	12-4	Final Exam	

Textbook: The textbook for this course is **mandatory.**
Mastering Kali Linux for Advanced Penetration Testing 2nd edition
ISBN 978-1-78712-023-5

Readings/Videos: Readings for the class will be assigned from the textbook as well as in the form of online reading. Online resources and videos will be linked from or embedded in a Blackboard page. It is essential that you do all readings and/or view the videos before coming to class on the assigned date. These materials are a necessary and integral part of the class and will form the basis for any class discussions on the topic. Specific readings are assigned by topic above.

Course Objectives: At the conclusion of this course, each successful student will able to:

- Explain the professional hacker's methodology for attacking a network.
- Explain the script kiddie's methodology for attacking network.
- Explain Network Security vulnerabilities.
- Explain Hackers, hacker techniques, tools and methodologies
- Describe hacker motivation, perform network reconnaissance and network scanning methods
- Describe and perform covering tracks after gaining access to a network.
- Describe the general symptoms of a virus attack
- Define and describe the two basic approaches to antivirus software.
- Describe how to defend against a worm and virus attack.
- Describe the steps in planning for a computer incident.
- Identify the difficulty is establishing who has jurisdiction over a computer crime.
- Understand the legal issues with regard to preserving digital evidence.
- Identify and describe the incident response goals and priorities.
- Describe the factors involved in identifying a computer incident.
- Describe and use the various tools associated with identifying an intruder.
- Describe how to handle and evaluate a computer incident.
- Recognize the role of law enforcement and rule of particularity in executing a search warrant.
- Describe the role the network security specialist would play in assisting the law enforcement and prosecution effort.
- Describe the difficulties in prosecuting a computer crime incident.
- Differentiate between competitive intelligence, economic intelligence, and industrial

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.

Guest Lectures: Guest lecturers may be featured as part of course topics. When a guest speaker is expected you should make an extra effort to be seated and ready prior to class time. Guest lectures may be in the evening in which case class will not be held during a scheduled morning period. A question & answer/ discussion period will be held at the end of each lecturer's presentation.

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 708-529-1563 prior to class time. Live section students who miss a class should always watch the lecture online.

Assignments: Individual assignments will be given about every week

Vulnerability Report:

A draft of your initial vulnerability report will be due on November 6. It should be the initial framework with some findings and be 3 or more pages in length

Vulnerability Report Final:

A completed report is due December 6th and should adhere to a framework and be at least 5 or more pages in length with descriptions and narratives.

Examinations: The final examination will consist of multiple choice, T & F 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 443/IT-S 443 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%

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

Draft Report	**25%**
Assignments	**25%**
Final Exam	**25%**
Final Report	**25%**

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.