MIS 5211 – Introduction to Ethical Hacking
Fall 2018

About the Instructor

William (Bill) Bailey
Email: william.bailey@temple.edu
e-profile: http://community.mis.temple.edu/members/william-bailey/
Office hours: by appointment

Class Location and Time

Classroom: WebEx:
https://foxsbm.webex.com/foxsbm/j.php?MTID=mf65cd585a923644684d3e4abc977861c
Time: Wednesday 5:30 pm – 8:00 pm (Philadelphia time zone)

Meeting number: 646 806 572

Meeting password: BSjYB4kP

Audio connection:
1-855-244-8681 Call-in toll-free number (US/Canada)
1-650-479-3207 Call-in toll number (US/Canada)
Global call-in numbers
Show toll-free dialing restrictions
Access code: 646 806 572

Class blog: https://community.mis.temple.edu/mis5211sec701fall2018/

Course Description:

This course introduces students to the hacking strategies and tactics used by ethical or "White Hat" hackers. Methods of vulnerability exploitation to be used primarily in the process of Security Penetration will be explored in theory and in hands on exercises. The course will require simple programming using Open Source scripting languages and hacking tool kits. For that reason some knowledge of and experience with computer programming is required.

Course Objectives:

In this course you will gain an understanding the process and tools used in Ethical Hacking and Penetration Testing. The Key subject areas that are covered in the course are:

1. How to structure a Penetration Test
2. Open Source tools used in Ethical Hacking and Penetration Testing
3. Commercial alternatives to Open Source tools

The first half of the course will focus on processes used to discover the structure and possible vulnerabilities in a target environment. The second half of the course will address the techniques and tools used to exploit weaknesses uncovered during the discovery phase.

Required Textbook and Readings

The materials for this course are drawn from multiple sources. There is no required textbook for this course. There are assigned readings throughout the course. These are available for free on the web.

These are the readings scheduled for the course. Through the semester, additional readings may be introduced during course discussions both in-class and on the community site.

	Reading
1	**Syllabus**
2	http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/2_Topolo.html
3	https://www.sans.org/reading-room/whitepapers/bestprac/open-source-reconnaissance-tools-business-partner-vulnerability-assessment-34490 http://www.sans.org/reading-room/whitepapers/auditing/the-art-of-reconnaissance-simple-techniques-60
4	http://www.sans.org/reading-room/whitepapers/auditing/proactive-vulnerability-assessments-nessus-78
5	http://www.sans.org/reading-room/whitepapers/auditing/footprinting-it-it-why-62?show=footprinting-it-it-why-62 http://www.sans.org/reading-room/whitepapers/testing/battle-for-the-internet-the-war-is-on-1075 Pages 9 to 11
6	http://www.sans.org/reading-room/whitepapers/networkdevs/packet-sniffing-switched-environment-244
7	http://www.sans.org/reading-room/whitepapers/tools/netcat-tcp-ip-swiss-army-knife-952
8	http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529
9	http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/1_Overvu.html
10	http://cdn.ttgtmedia.com/rms/pdf/SearchSecurity.in_Burp_%20Suite_tutorial_Part_01.pdf http://cdn.ttgtmedia.com/rms/pdf/SearchSecurity.in_Burp_%20Suite_tutorial_Part_02.pdf http://cdn.ttgtmedia.com/rms/pdf/SearchSecurity.in_Burp_%20Suite_tutorial_

	Reading
	Part_03.pdf We will only use the functionality discussed in the first paper http://www.sans.org/reading-room/whitepapers/application/web-application-injection-vulnerabilities-web-app-039-s-security-nemesis-34247 http://www.sans.org/reading-room/whitepapers/application/web-application-security-for-managers-27 The last two papers also contain information applicable to the following week.
11	http://sec4app.com/download/SQL_Injection_Tutorial.pdf
12	http://www.sans.org/reading-room/whitepapers/services/web-services-security-overview-225 http://www.sans.org/reading-room/whitepapers/securecode/xml-web-services-security-web-based-application-security-1201
13	http://www.sans.org/reading-room/whitepapers/intrusion/beating-ips-34137

Assignments

The readings, weekly discussion questions and case study assignments have been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts. Your participation in the online and class discussions is critical. Evaluation is based on you consistently demonstrating your engagement with the material. Assessment is based on what you contribute. The **frequency** and **quality** of your contributions are equally important.

Answers to Weekly Reading Discussion Questions: Each Friday morning, you will find a post that includes several discussion questions about the coming week's readings. You will be expected to post your answer to one of the discussion questions on the week's readings by **Sunday @11:59 PM.** A paragraph or two of thoughtful analysis is expected for your initial answer to the question. Post your answer to the weekly class assignment blog. You must come to class prepared to discuss all of these questions in detail when we meet.

Participation

Much of your learning will occur as you prepare for and participate in discussion about the course material. The assignments, cases, and readings have been carefully chosen to bring the real work into class discussion while also illustrating fundamental concepts. Your participation in the online and class discussions is critical. Evaluation is based on you consistently demonstrating your engagement with the material. Assessment is based on what you contribute. The frequency and quality of your contributions are equally important.

Therefore, in addition to fulfilling your weekly assignment by actively participating in class and posting your answer to one of the reading discussion questions, each week you are also expected to participate in the dialogue with other responses to the Weekly Reading Discussion Questions.

Comments on Other student's answers and comments to weekly reading discussion questions: Read the responses of others to the discussion questions and contribute at least four (4) substantive posts that include your thoughtful comments as you participate in the discussion of the questions. The posting of these additional four comments is due by **Wednesday @ 11:59am**.

Exercise Analyses

You will officially prepare three analyses reports that are assigned during the semester. For each assignment students are to break into groups and work together to prepare a one to two page report and a presentation of no more than four slides for presentation in the following class. Your analysis should not exceed one single-spaced page using 11 point Times New Roman font with one-inch margins. Do not prepare a separate cover page, instead put your name, the class section number (MIS5211.701), and the analysis in the top-left corner of the header.

To submit your analysis, you must post it on the class blog no later than Tuesday at 8:00 AM of the week it is due. Please copy your analysis in clear text onto the blog.

Late submissions for this deadline will result in no credit earned for this assignment.

There is no one particular style for a good analysis. But, there are some common elements to excellent submissions (additional, grade-specific criteria are provided at the end of this syllabus):

- The opening of the analysis makes it immediately clear which assignment and what question is being addressed.
- You have cited specific details regarding key facts and issues of the case. Instead of general observations about information technology or organizations that apply to any problem, draw details from the assignment itself. Analyses, observations, and suggestions should be tied directly to those key facts and issues. You can also draw on the other readings in the course to inform and support your arguments.
- After analyzing the details of the analysis, discuss how its specific issues have broader application. In other words, use your analysis to provide some advice to managerial decision-makers that can be applied to other situations beyond this case.
- Provide a well-balanced perspective. For example, when making a recommendation explain the pros and cons, providing both the rationale (the why) as well as its feasibility (the how). Well-considered recommendations

include discussion of potential issues with your solution and conditions that should be in place for your recommendation to be successful.

Group Project Report and Presentation

The individual and group projects are related. Your individual project will contribute to your team project effort. Therefore, coordination is required in choosing topics for both projects. A detailed description of the assignment will be posted to the class website. Students may choose their own groups of about five members each. Because group work requires close coordination, I strongly recommend considering compatibility in availability (e.g., work and class schedules, work and home locations, and other constraints) before finalizing group membership. Refer to the schedule for project deliverable dates.

Quizzes

Through the course, there will be periodic quizzes that consist of multiple choice questions modeled after the content of certification exams such as the CISA, CISSP, or other certifications such as OSCP or CEH. The quizzes give you practice answering time-bound questions, help you gain skills that improve your test-taking abilities, and help highlight areas requiring additional study and attention. The quizzes are a portion of the final grade.

Exams

There will be two in-class exams given during the semester. Together these exams are weighted 30% of your final grade.

All exams will consist of multiple-choice, fill in the blank and possible short answer questions. You will have a fixed time (e.g. 40 minutes) to complete the exam. Exam 1 will occur during week 7, and Exam 2 will occur during week 14. In general, the exams will not be cumulative but focused on the course materials since the beginning of last exam. However, some concepts highlighted in class as important or a 'Core Principle' may appear on either or both exams.

A missed exam can only be made up in the case of documented and verifiable extreme emergency situations. No make-up is possible for Exam 2.

Weekly Cycle

As outlined above in the **Assignments and Participation** sections, much of your learning will occur as you prepare for and participate in discussions about the course content. To facilitate learning the course material, we will discuss course material on the class blog in between classes. Each week this discussion will follow this cycle:

When	Actor	Task	Type
Friday	Instructor (me)	Post reading questions (Friday am)	
Sunday 11:59 pm	Student	Post answers to reading questions	Assignment
Sunday 11:59 pm	Student	Complete Quiz (if applicable)	Assignment
Wednesday 9:00 am	Student	Post case study analysis (when due)	Assignment
Wednesday 11:59 am	Student	Post 4 comments to others' answers	Participation
Wednesday 5:30 pm-8 pm	Both of Us	Class meeting via Webex	Participation
Thursday	Instructor	Post summary notes (if any)	

Evaluation and Grading

Item	Weight
Analyses Reports (3)	30%
Discussion Questions	15%
Participation	10%
Quizes	15%
Exams	30%
	100%

Grading Scale			
94 – 100	A	73 – 76	C
90 – 93	A-	70 – 72	C-
87 – 89	B+	67 – 69	D+
83 – 86	B	63 – 66	D
80 – 82	B-	60 – 62	D-
77 – 79	C+	Below 60	F

Grading Criteria

The following criteria are used for evaluating assignments. You can roughly translate a letter grade as the midpoint in the scale (for example, an A- equates to a 91.5).

Criteria	Grade
The assignment consistently exceeds expectations. It demonstrates originality of thought and creativity throughout. Beyond completing all of the required elements, new concepts and ideas are detailed that transcend general discussions along similar topic areas. There are no mechanical, grammatical, or organization issues that detract from the ideas.	A- or A
The assignment consistently meets expectations. It contains all the information prescribed for the assignment and demonstrates a command of the subject matter. There is sufficient detail to cover the subject completely but not too much as to be distracting. There may be some procedural issues, such as grammar or organizational challenges, but these do not significantly detract from the intended assignment goals.	B-, B, B+
The assignment fails to consistently meet expectations. That is, the assignment is complete but contains problems that detract from the intended goals. These issues may be relating to content detail, be grammatical, or be a general lack of clarity. Other problems might include not fully following assignment directions.	C-, C, C+
The assignment constantly fails to meet expectations. It is incomplete or in some other way consistently fails to demonstrate a firm grasp of the assigned material.	Below C-

Late Assignment Policy

An assignment is considered late if it is turned in after the assignment deadlines stated above. No late assignments will be accepted without penalty unless arrangements for validated unusual or unforeseen situations have been made.

- Class Blog contributions cannot be turned in late. If you miss contributing prior to class for that week's discussion / questions you will receive no credit for it.
- The exercise assignments will be assessed **a 20% penalty** each day they are late. No credit is given for assignments turned in over five calendar days past the due date.

- You must submit all assignments, even if no credit is given. **If you skip an assignment, an additional 10 points will be subtracted from your final grade in the course.**
- Plan ahead and backup your work. ***Equipment failure is not an acceptable reason for turning in an assignment late.***

Citation Guidelines

If you use text, figures, and data in reports that were created by others you must identify the source and clearly differentiate your work from the material that you are referencing. If you fail to do so you are plagiarizing. There are many different acceptable formats that you can use to cite the work of others (see some of the resources below). The formats are not as important as the intent. You must clearly show the reader what is your work and what is a reference to someone else's work.

Plagiarism and Academic Dishonesty

All work done for this course: papers, examinations, homework exercises, blog posts, laboratory reports, oral presentations — is expected to be the individual effort of the student presenting the work.

Plagiarism and academic dishonesty can take many forms. The most obvious is copying from another student's exam, but the following are also forms of this:

- Copying material directly, word-for-word, from a source (including the Internet)
- Using material from a source without a proper citation
- Turning in an assignment from a previous semester as if it were your own
- Having someone else complete your homework or project and submitting it as if it were your own
- Using material from another student's assignment in your own assignment

Plagiarism and cheating are serious offenses, and behavior like this will not be tolerated in this class. In cases of cheating, both parties will be held equally responsible, i.e. both the student who shares the work and the student who copies the work. Penalties for such actions are given at my discretion, and can range from a failing grade for the individual assignment, to a failing grade for the entire course, to expulsion from the program.

Student and Faculty Academic Rights and Responsibilities

The University has adopted a policy on Student and Faculty Academic Rights and Responsibilities (Policy # 03.70.02) which can be accessed through the following link: http://policies.temple.edu/getdoc.asp?policy_no=03.70.02

Additional Information

Availability of Instructor	▪ Please feel free to contact me via e-mail with any issues related to this class. I will also be available at the end of each session. Please note that these discussions are to address questions/concerns but are NOT for helping students catch up on content they missed because they were absent. Note: I will respond promptly when contacted during the week ▪ I am available to meet personally with you: ✓ Immediately after class ✓ By appointment prior to class ✓ By appointment by phone
Attendance Policy	▪ Class discussion is intended to be an integral part of the course. Therefore, full attendance is expected by every student. ▪ If you are absent from class, speak with your classmates to catch up on what you have missed.
Class Etiquette	▪ Please be respectful of the class environment. ▪ Class starts promptly at the start time. Arrive on time and stay until the end of class. ▪ Turn off and put away cell phones, pagers and alarms during class. ▪ Limit the use of electronic devices (e.g., laptop, tablet computer) to class-related usage such as taking notes. Restrict the use of an Internet connection (e.g., checking email, Internet browsing, sending instant messages) to before class, during class breaks, or after class. ▪ Refrain from personal discussions during class. Please leave the room if you need to speak to another student for more than a few words. If a student cannot refrain from engaging in private conversation and this becomes a pattern, the students will be asked to leave the classroom to allow the remainder of the students to work. ▪ During class time speak to the entire class (or breakout group) and let each person "take their turn." ▪ Be fully present and remain present for the entirety of each class meeting.

Course Schedule

Week	Topic	Assignments
1	Overview of Course, Philosophy of Ethical Hacking and Penetration Testing, and the hacking process	Quiz
2	TCP/IP and Network Architecture and its impact on the process of hacking. Google Hacking	Quiz
3	Reconnaissance – Concepts of reconnaissance used to obtain basic, high level information about a target organization, often considered information leakage, including but not limited to technical and non-technical public contacts, IP address ranges, document formats, and supported systems.	Quiz
4	Vulnerability scanning and analysis of results Assignment presentation	Quiz
5	Nessus	Quiz
6	Sniffers	Quiz
7	Netcat Hellcat	Exam
8	Social Engineering, Encoding, and Encryption	Quiz
9	Malware including Trojans, Backdoors, Zero-days, Virus, Worms, and Polymorphic malware	Quiz
10	Web application hacking, Intercepting Proxies, and URL Editing	Quiz
11	SQL injection Assignment presentation	Quiz Intercepting Proxy exercise targeted against a public website of your choice. Only normal website activity is to be profiled. **Under no circumstances shall injection techniques be used.**
12	Web Services	Quiz
13	Evasion Techniques	Quiz
14	Review of all topics and wrap up discussion	Exam

Notes on Course Recordings

Courses will be hosted and recorded using Webex. The link(s) to the recordings will be distributed and/or published.

Acknowledgements

This syllabus represents the collaborative efforts of MIS Department Professors Schuff, Lanter, Mackey, Weinberg, Yoo, and Johnson.