Spring 2017

About the Instructor:

Wade Mackey (wade.mackey@temple.edu)
http://community.mis.temple.edu/rflanagan/
Phone: 717-682-2925
Office hours: (by appointment)

Class Location and Time:

Online TBD

Course Description:

This course introduces students to Penetration Testing. Methods of vulnerability assessment and exploitation are examined as a means of identifying areas requiring improved security and recommended changes. The ethical, business governance and legal implications of penetration testing are examined. Specific techniques are examined in detail with the intent of giving the students a practical understanding of how Penetration Tests are conducted and laboratory-based experience in their actual conduct.

Course Objectives:

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

1. Utilization of the MetaSploit Framework in penetration testing
2. Web Application Hacking with Intercepting Proxies and the WebGoat application
3. Wireless Security and techniques to break wireless security

Required Text 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.

Evaluation and Grading

Item	Weight
Participation (in class and online)	20%
Analyses Reports (3)	30%
Exams (2)	50%

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

Participation

Much of your learning will occur as you prepare for and participate in discussions about the course material. The assignments, analysis, and readings have been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts.

To encourage participation, 20% of the course grade is earned through preparation before class, and participation during and between classes. Evaluation is based on a consistent demonstrated engagement with the process of learning. Assessment is based on what you contribute, not simply what you know.

1) **Participation between classes** – To facilitate learning the course material, we will also discuss course material on the class blog in between classes. Each week, I will post a discussion question or two on the class blog for the following week's topic. The question will relate to the assigned readings, a topic to be discussed in class, or a relevant current event. Reading and commenting on these analyses will contribute to the quality of our in-class discussions.

   Every student is expected to contribute to the online class discussion at least four times each week. Online contributions will be graded on both the quality of your submissions and the overall quantity. Four substantive posts a week will be considered a B.

2) **Participation during class** – We will typically start each discussion with "opening" questions about the assigned readings and analysis. I may ask for volunteers, or I may call on you. Students called on to answer should be able to summarize the key issues, opportunities, and challenges in the case study. All students should be prepared to answer these questions.

Another important aspect of in-class participation is completion of in-class assignments and contribution to break-out group activities.

The criteria for class participation includes attendance, punctuality, level of preparation, professionalism, answering questions, discussing readings, discussing case studies, contributing to group activities, and contributing to a positive learning environment.

Exercise Analysis

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 (MIS5212.001), 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 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.

Exams

We will have 3 multiple choice question exams. The first one will cover MetaSploit and will comprise 15% of your final grade. The second exam will cover Web Application Hacking Techniques and will comprise 15% of your final grade. The third exam will cover wireless security and include some comprehensive questions from earlier tests and is weighted 20% of your final grade.
There will be both a midterm exam final exam for this course. Both exams will be comprised of short-answer and/or longer open-ended questions. Check the schedule for dates.

A missed exam can only be made up in the case of documented and verifiable extreme emergency situations.

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.

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.

- The project management simulation and individual report 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.
- Case analyses cannot be submitted late under any circumstances. If you miss the deadline, you'll need to choose another case study to submit.
- 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.**

- Weekly write-ups cannot be turned in late. If you miss the deadline you will receive no credit for it, although the additional 10 point grade penalty does not apply here.
- Plan ahead and backup your work. ***Equipment failure is not an acceptable reason for turning in an assignment late.***

Classroom Etiquette

The environment you and your fellow students create in class directly impacts the value that is gained from the course. To that end, the following are my expectation of your conduct in this class:

- Arrive on time and stay until the end of class.
- Turn off cell phones, pagers and alarms while in 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.
- 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.

Citation Guidelines

If you use text, figures, and data in reports that was 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

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=03.70.02http://policies.temple.edu/getdoc.asp?policy_no=03.70.02 http://policies.temple.edu/getdoc.asp?policy_no=03.70.02

Grading Criteria

The following are the criteria 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+

e 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-

Readings

Readings	
2	http://www.offensive-security.com/metasploit-unleashed/Main_Page Review Fundamentals, Information Gathering, and Vulnerability Scanning Read Exploit Development, Web App Exploit Development, Client Side Attacks and Auxiliary Module Reference
3	http://www.offensive-security.com/metasploit-unleashed/Main_Page Read MSF Post Exploitation, Meterpreter Scripting, Maintaining Access
4	http://www.offensive-security.com/metasploit-unleashed/Main_Page Read MSF Extended Usage and Metasploit GUIs
5	No Reading Assignment
6	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_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
7	http://sec4app.com/download/SQL_Injection_Tutorial.pdf
8	No Reading Assignment
9	https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs https://www.wireshark.org/docs/wsug_html_chunked/ChapterUsing.html (Look through chapter so you are familiar with what you can find)
10	No Reading Assignment
11	http://en.wikipedia.org/wiki/IEEE_802.11 https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx
12	http://aircrack-ng.org/doku.php?id=getting_started
13	No Reading Assignment

Schedule

Date	Topic	Assignments
1 Full	Course Introduction, Introduction to the Metasploit Framework including Basics, Intelligence Gathering, Vulnerability Scanning, and Exploitation	
2 1 hr	Meterpreter, Avoiding Detection, Client Side Attacks, and Auxiliary Modules	Quiz
3 1 hr	Social Engineering Toolkit, SQL Injection, Karmetasploit, Building Modules in Metasploit, and Creating Exploits	Quiz
4 1 hr	Porting Exploits, Scripting, and Simulating Penetration Testing Ettercap	Quiz
5 Full	Test 1, Introduction to OWASP's WebGoat application	Test 1
6 Independent Study	Unvalidated Parameters, Broken Access Control, and Broken Authentication	Quiz Analysis Report: Learnings from Metasploit run against a publically available VM the student chooses
7 1 hr	Cross Site Scripting, Injection Flaws, Error Handling, and Insecure Storage	Quiz
8 1 hr	Denial of Service, Configuration Management, and Web Services	Quiz
9 1 hr	Ajax Security and an Introduction to the WebGoat Challenge Wireshark	Quiz
10 1 hr	Test 2, Introduction to Wireless Security	Test 2
11 Full	Wireless Recon, WEP, and WPA2	Quiz Analysis Report: Learnings from the WebGoat Challenge
12 1 hr	WPA2 Enterprise, Wireless beyond WiFi	Quiz
13 Full	Cain and Able	Quiz
14 Full	Review of all topics and wrap up discussion	Test 3

Acknowledgements

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