University of Rhode Island
Department of Computer Science and Statistics
Digital Forensics and Cyber Security Center

CSF 538 Penetration Testing
CSC 492 Special Topics in Computer Science

Summer 2015 Syllabus

Instructor: Stephen Jaegle (jaegles@cs.uri.edu)

Teaching Assistant: Nicholas Giannini (ngiannini@my.uri.edu)

Course Meets: Online

Course Web Site: https://sakai.uri.edu/

Course Goals:

- Learn about the field of Penetration Testing, by building on those topics learned in CSF 432, Network and Systems Security
- Learn the process of a Penetration Testing engagement
- Learn in-depth details about the Kali Linux platform and the attacks available to a penetration tester
- Learn about tools and techniques for testing and exploiting Windows and Linux platforms
- Gain hands–on experience with Penetration Testing tools
- Conduct independent research on a specific area of penetration testing (CSF 538 Grad only)

Course Materials:

Textbook:

- *Penetration Testing: A Hands-On Introduction to Hacking* by Georgia Weidman. ISBN: 978-1-59327-564-8

Hardware and Software Requirements:

- Penetration Testing and special purpose software provided through Sakai.

Course Work:

This is an online course that can be completed from anywhere with a computer and Internet connection. The course involves the use of a forum, video lectures, readings, assignments, and quizzes that are organized into Weekly Lessons and can be accessed from the course website. For this course, you should expect to complete between 15 - 20 hours worth of coursework each week.

Lectures

There are lectures each week that can be accessed from the Lessons pages of the course website. Lectures will generally be posted on Fridays. Students are expected to view all lectures, ask questions about them on the discussion board as necessary, participate in discussions about the lectures, and be able to answer quiz questions about them.

Readings

Readings will be assigned every week. Readings will be referred to and discussed throughout course lectures and assignments. Students are expected to do all readings, ask questions about them on the discussion board as necessary, participate in discussions about the readings, and be able to answer quiz questions about them.

Assignments

Assignments will generally be posted on Friday for the coming week and be due by 11:55pm the Monday after the following weekend, i.e., about 10 days later, unless otherwise specified. Assignments submitted after the due date will receive a 5% late penalty per day. No exercise reports will be accepted later than 4 days past the due date. In addition, teaching staff will not be available to offer assistance on an exercise past its due date.

Pen Testing Assignments - There are penetration testing exercises where students are required to perform various pen testing tasks. Material required for the exercises are provided via download or on a course DVD that is U.S.-mailed to students. Most exercises will require the use of software provided as part of the course, or a trial version that you will need to download from external web sites as specified. Some exercises will require the use of virtual machines, using configurations that will be provided in the course materials.

Assignment Submission - Adherence to the form specified in exercise descriptions is expected and constitutes part of the grade for each assignment.

Since this course meets online, any questions regarding the material being covered, assignments, etc., should be posted on the discussion board so that the instructor, TA, and other students who may know the answer or have the same questions may provide a response in a timely manner. Questions regarding your grades can be emailed directly to the instructor or TA.

Quizzes

Each week, there will be a quiz based on all reading and lecture material for that week. Quizzes will be available for three days (typically Thursday through Saturday) of the week that the topic is being covered. Your single lowest required quiz grade of the term will be dropped.

Discussions

The course discussion forums serve not only as graded discussion forums (Mandatory Discussions), but also as a way for the instructors to make course announcements (Info topics) and for students to post questions about the course readings, lectures and assignments (Question topics).

Info topics - These discussion topics are typically posted by the Professor or TA to clarify or update some information on the course, an assignment, or some other relevant topic of interest.

Question topics - These discussion topics are typically posted by students seeking help from other students and/or from the staff about some aspect of the course or about computer forensics in general. Participation in these discussion topics is optional and not required, although particularly helpful responses to the questions of others can help your class participation grade.

Mandatory Discussions - (indicated by [Mandatory] in the discussion topic title). Because this is an online course, the Mandatory discussions will form an integral part of your participation grade. Mandatory discussions will be posted by the Professor, TA, URI staff and also Graduate students as part of their assigned research topics. Late posts will not be graded. Missed graded discussions can only be made-up in exceptional circumstances, such as death in the family or documented illness.

Your posts should demonstrate that you understand the materials assigned and may integrate multiple views and/or motivate other students to respond. You should provide evidence that you are reading other postings and bring out interesting interpretations. In short, go beyond just demonstrating that you know the facts, and show that you are able to analyze them and handle conceptual ideas. Posts that only state, "I agree" or "That is an interesting idea" are acceptable in the forum, but they will not receive credit. Feel free to contribute from your personal experiences or your own research or interests.

The participation grade is based partly on actively participating in the class discussion board by:

1. Adding substantive responses and counter responses to the mandatory discussion questions that show thought, research, and understanding of the topic being discussed;

2. Assisting other students with help/guidance; and/or

3. Contributing to the class by posting online resources relating to topics from the course.

All discussion is considered confidential within the course – content posted on the course

discussion board is not to be shared with people outside of the course. All class discussion should be on the class discussion board, direct student-to-student contact is not allowed unless approved by the instructor.

Final Exam

There will be a final exam during the final week of the course. The exam will be cumulative and will require you to put into practice everything you have learned in this course.

Graduate Research Topic:

- You will be assigned a topic relating to a Penetration Testing and Exploitation application. You will be responsible for conducting research on the assigned topic and then developing a comprehensive paper on your topic.
- You will be responsible for conducting your own in-depth testing and research on the application and explaining to the class how to conduct an investigation or exploitation of this area using various tools and techniques you discover through your research.
- Note: As you begin research, you will start posting your findings to the class, to facilitate discussion on your topic. The tools and techniques you discuss may very well be useful to others conducting similar analysis on topic. You will be using the discussion board extensively, not only to facilitate discussion on your topic, but to also participate in discussions with the other CSF 538 students on their topic and share ideas and findings.

Topics:

A suggested list of topics and a selection process will be part of the assignments in Sakai.

Typical Weekly Schedule:

Our typical assignment week runs from Friday to Monday after the following weekend (about 10 days).

- New readings, lectures, and assignments posted for the week on Friday.
- Quiz (available Friday-Monday) on the readings and lectures that were assigned the previous Friday.
- Assignments due by midnight (US Eastern time) on Monday.

Discussion Board Use & Teaching Staff Availability:

Any question related to the material covered, troubleshooting, or not understanding assignments should be directed to the discussion board so that the instructor, TA, and other students who may know the answer or have the same questions may provide a response in a timely manner. The teaching staff are happy to answer questions on the discussion forum, and due to our own work schedules, we are not online 24x7 so we may not respond to electronic questions immediately, but we will reply within 24 hours. Owing to the asynchronous nature of forum communication, waiting until the last minute to post questions is not advisable. We encourage you to continue to use the discussion board for help from each other.

You should contact the teaching staff via email with questions related to grading issues or homework questions that cannot be posted to the discussion board, such as questions that give away the answer to an assignment. You should not contact the teaching staff via email with general questions related to troubleshooting or not understanding homework assignments.

If you would like to schedule an online or in-person appointment to meet with teaching staff you may do so by contacting them via email. These appointments should be made with a minimum of 24 hrs notice.

The teaching staff will not offer help on an assignment at any time, through any means (discussion board, email, in person) after noon on the Friday that the assignment is due. In addition, no assistance will be provided for past-due assignments.

Grading:

Grades will be determined according to these weights:

	CSF 538	CSC 492
Quizzes:	15%	20%
Assignments:	35%	35%
Graduate Project:	20%	0%
Final Exam:	20%	25%
Class Participation:	10%	20%

Feedback on quizzes, exams, and exercises will either be available on the course web site, emailed to you or placed in your submit folder. You have one week from the posting of a grade to submit any concern about that grade, in email to the TA. Concerns expressed after one week from posting will not be considered.

Tentative Schedule of Topics by Week:

Week 1 – Introduction and Setting up your Lab

Week 2 – Exploring Kali Linux and PenTest Programming

Week 3 – Exploring Metasploit and Network Traffic Attacks

Week 4 – Information Gathering and Finding Vulnerabilities

Week 5 – Exploitation and Password Attacks

Week 6 – Social Engineering and Bypassing AV Applications

Week 7 – Post Exploitation & Web and Wireless Attacks

Week 8 – Buffer Overflow and Exception Handling

Week 9 – Fuzzing

Week 10 – Final Exam (Practical)

Disability Accommodations

Any student with a documented disability is welcome to contact me as early in the semester as possible so that we may arrange reasonable accommodations. As part of this process, please be in touch with the Disability Services for Students Office at 330 Memorial Union, (401) 874-2098.

Academic Integrity

Assignments are to be the result of your individual efforts, unless you are told otherwise. It is easy to copy material on the computer; such copying constitutes plagiarism and will earn a 0 on the assignment. In some cases, a charge of plagiarism may result in a failure of the course. Additionally, the charge of academic dishonesty will go on your record in the Office of Student Life. If you need help with an assignment, or are not sure if something is acceptable, discuss it with a staff member.

Ethics

Tools and programs that can be used to break or "hack" into systems should only be used in an ethical, professional and legal manner. This means that they should only be used to test the current strength of security networks that are your own or those that you have explicit written consent from the owner of the systems, so that proper improvements can be made. The knowledge presented here is not intended for use in any illegal capacity and is meant to aid learning and development of Cyber Security and Information Technology practices and concepts only.