CSEC 759: Graduate Seminar – Enterprise Penetration Testing
Section 01
Spring 2019

Instructor	Rob Olson
Office Location	2118 GOL
Phone	585-475-4601
E-mail	rboics@rit.edu
Office Hours	TBD
Course Time	T/TH 9:30-10:45
Course Place	GOL-3445

1. Catalog description: Negotiating a contract, performing a penetration test, and presenting the results will be examined and exercised. Students will be exposed to tools and techniques employed in penetration testing. The challenges and precautions necessary in planning for and conducting an assessment at an enterprise level exposing potential vulnerabilities are studied. After a penetration testing exercise, the students will develop a coherent and comprehensive report of their findings to present to their client. Special focus will be on the impact of the findings on the security of the client.

2. Prerequisite(s):

Graduate standing

3. Course Textbook:

None, but there may be supplemental reading provided on a week-by-week basis.

4. Reference Materials:

- Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman, No Starch Press, 2014
- **Grey Hat Hacking: The Ethical Hacker's Handbook 5th edition, Regaldao et al., McGraw-Hill Education, 2017**
- **Black Hat Python: Python Programming for Hackers and Pentesters, Justin Seitz, No Starch Press, 2014**
- Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm, Syngress 2009

4. Course Objective: This course will teach students many skills, both technical and non-technical, that they will need to execute and manage penetration tests. A particular emphasis will be placed on soft skills related to penetration testing, penetration test planning, tool development *before* tool usage, and producing actionable results for clients.

5. Course Structure

- Lectures/Demonstrations
- Simulated penetration tests
- Weekly presentations

6. *Tentative* Course Outline:

Week 1:	Intro, Legal and ethics, penetration testing process, documentation
Week 2:	Pre-engagement activities, penetration test planning, and operational security
Week 3:	Reconnaissance and OSINT
Week 4:	Network enumeration and vulnerability scanning
Week 5:	Web exploitation
Week 6:	Network exploitation and pivoting
Week 7:	Exploits and exploit development
Week 8:	Exploiting system misconfigurations remotely
Week 9-10:	Privilege escalation techniques
Week 11-12:	Post-exploitation data collection
Week 13-14:	Optimizing penetration test output

7. Grading:

The relative weight of each component of your grade is shown on the table below.

Component	**Percentage**
Weekly Progress Reports/Presentations	30%
Peer Evaluations	10%
Penetration Test Report 1 (Including Pres.)	20%
Penetration Test Report 2 (Including Pres.)	40%

The table below lists student's grade for a given percentage achieved.

94%-100%	90%-93%	88%-89%	82%-87%	80%-81%	78%-79%	72%-77%	70%-71%	60-69	0%-59%
A	A-	B+	B	B-	C+	C	C-	D	Fail

8. Exams, Projects, and Labs/Assignments:

All exams must be taken on the day that they are given. All projects and lab assignments are due on the date listed in the hand-out provided by the instructor. No exceptions will be made, except for excused

absences. Excused absences will be granted for the reasons such as the following and require written documentation:

1. Illness of the student or serious illness of a member of the student's immediate family.
2. A death in the student's immediate family
3. Trips sponsored by official RIT student groups, academic units, or athletic teams.
4. Major religious holidays

A student requiring special considerations for reasons 3 or 4 should talk to the instructor at least a week in advance, whenever possible.

9. Class Attendance

Attendance is highly recommended. The students are responsible for all material presented in class and in assigned reading. If a student misses a class, it is their responsibility to obtain the lecture information, including announcements, from fellow students. Make-up lectures will not be given. You are responsible for all information from each lecture whether or not the lecture was attended.

10. Academic Honesty

The following is taken from the RIT policy on academic honesty[1]:

> "A breach of student academic integrity falls into three basic areas: cheating, duplicate submission and plagiarism
>
> A. Cheating: Cheating is any form of fraudulent or deceptive academic act, including falsification of data, possessing, providing, or using unapproved materials, sources, or tools for a project, exam, or body of work submitted for faculty evaluation.
>
> B. Duplicate Submission: Duplicate submission is the submitting of the same or similar work for credit in more than one course without prior approval of the instructors for those same courses.
>
> C. Plagiarism: Plagiarism is the representation of others' ideas as one's own without giving proper attribution to the original author or authors. Plagiarism occurs when a student copies direct phrases from a text (e.g. books, journals, and internet) and does not provide quotation marks or paraphrases or summarizes those ideas without giving credit to the author or authors. In all cases, if such information is not properly and accurately documented with appropriate credit given, then the student has committed plagiarism."

Potential punishments for academic dishonesty may include:

[1] The policy on academic honesty can be found at https://www.rit.edu/academicaffairs/policiesmanual/d080

- Receiving a failing grade on an assignment
- Failing the course
- Dismissal from the university

11. Responsible Disclosure

During the course of the semester, students in CSEC 759 may uncover previously unknown security vulnerabilities in mobile applications or mobile devices. In the event that this happens, students will be expected to practice responsible disclosure practices. This includes, but may not be limited to, submitting the vulnerability to a bug bounty program or notifying the company of the vulnerability far enough in advance of releasing details to give the company sufficient time to respond. The instructor reserves the right to penalize a students' grade if the student fails to practice responsible disclosure and to recommend the student for further academic discipline if needed.