CSEC 465: Network and System Security Audit
Section 01
Fall 2018

Instructor	Prof. Robert Olson
Office Location	GOL 2118
Phone	475-4610 (Please Don't Call Me)
E-mail	rboics@rit.edu
Office Hours	T/TH 11:30-1:00
Course Time	MWF 10:00 – 10:50
Course Place	GOL-1445

1. Catalog description: This course will provide students with an introduction to the processes and procedures for performing a technical security audit of systems and networks. Students will explore available auditing techniques and apply appropriate tools to audit hosts, servers and network infrastructure components. In addition, students will **write and present** their audit reports on vulnerability analysis.

2. Prerequisite(s):

NSSA-221 and NSSA 241

3. Required Course Textbook: None

4. Course Objective: This course is designed to teach students processes and procedures of system and networks audits and develop students' ability of applying appropriate tools to conduct technical auditing.

5. Learning Outcomes:

After completing this course, the student will be able to:

- Explain the fundamental techniques, processes, and procedures of network and system audits. Accessed through labs and exams.
- Describe the basic design and configuration of routers, firewalls, and intrusion detection systems. Assessed through labs and exams.
- Identify and apply appropriate tools to perform systems (Unix/Windows) and network infrastructure components audit. Assessed through labs.
- Utilize available tools to conduct vulnerability and validation testing. Assessed through labs.
- Write and present an auditing report on security vulnerability. Assessed through labs.

6. Tentative Course Outline:

Week 1:	Intro to Security Auditing and Audit Process	
Week 2:	Threat Modeling and Risk	Lab 1: Threat Modeling
Week 3:	Security Policy and Audit Planning	Lab 2: Policy Writing
Week 4:	Asset Management and Discovery	Lab 3: Net Discovery/System Audit
Week 5-6:	Auditing at Scale	
Week 6-7:	System and Network Service Auditing	Lab 4: Auditing at Scale
Week 7:	Mid-term Exam	
Week 8:	Vulnerability mgmt/scanning	Lab 5: Vuln Scanning
Week 9-10:	Penetration Testing	Lab 6: Penetration Test
Week 11-12:	Social and Physical Security Auditing	
Week 12-13:	Software Vulns & Source Code Audits	Lab 7: Source Code Auditing
Week 13-14:	Cloud Security and Auditing	Lab 8: AWS/Azure Auditing (Tentative)

7. Grading:

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

Component	**Percentage**
Lab Assignments [7-8]	40% (5% each)
Lab Group Peer Evaluations [4]	10% (2.5% each)
Lab Group Presentations [2]	20% (5% each)
Exams [2]	30% (15% each)

The table below lists student's grade for a given percentage achieved. Numeric grades that fall between categories will be rounded up or down at the discretion of the instructor.

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.

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. **You should not assume that PowerPoint presentations or demonstration notes will be posted on MyCourses.**

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:

- Receiving a failing grade on an assignment

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

- Failing the course
- Dismissal from the university

11. Responsible Disclosure

During the course of the semester, students in CSEC 465 may uncover previously unknown security vulnerabilities. In the event that this happens, students will be expected to follow 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 student’s grade if the student fails to practice responsible disclosure and to recommend the student for further academic discipline if needed.