CSEC 5/69: Cyber Operations & Adversary Emulation
Section 02
Spring 2022

Instructor	Prof. Robert Olson
Office Location	**Main CSEC Office Suite**
Phone	585-475-4601 (My office) * - Preferred
E-mail	rboics@rit.edu
Office Hours	T 2:00-3:30
Course Time	T/TH 9:30 – 10:45
Course Place	GCI-2750

1. CSEC 559 Catalog description: This course will provide students with the technical foundations necessary to construct custom tooling needed to perform offensive cyber operations or adversary emulation projects. Students will study, analyze, and implement access, persistence, and evasion techniques used by real advanced persistent threat actors. The design and implementation of malicious implants, command and control frameworks, and custom access will all be studied. This is a programming intensive course and students are expected to have familiarity with writing buffer overflow exploits.

CSEC 659 Catalog description: This course will provide students with the technical foundations necessary to construct custom tooling needed to perform offensive cyber operations or adversary emulation projects. Students will study, analyze, and implement access, persistence, and evasion techniques used by real advanced persistent threat actors. The design and implementation of malicious implants, command and control frameworks, and custom access will all be studied. Students will study cases of real-world cyber operations to both identify relevant technical details and analyze the strategic objective of the operation. Both international and domestic threat actors will be studied. This is a programming intensive course and students are expected to have familiarity with writing buffer overflow exploits.

2. Prerequisite(s):

CSEC 559: (CSEC 380 or SWEN 331) & CSCI 462
CSEC 659: CSEC 604 & CSEC 742

3. Course Textbook: None – resources will be made available via MyCourses

4. Course Learning Outcomes:
After completing this course, the student will be able to:

1. Students will be able to plan and develop implants which use common persistence and AV evasion techniques.
2. Students will be able to compare and contrast commonly used command and control frameworks.
3. Students will be able to plan and implement a custom command and control system.
4. Students will be able to describe and construct mechanisms for infecting a system with an implant.
5. (CSEC 659 only) Students will be able to deconstruct modern cyber operations, identify relevant technical details, and formulate hypotheses regarding relationship between the operation and public policy.

5. Program Learning Outcomes:
After completing this course, the student will be able to:

- Apply the theory and principles of computing security
- Demonstrate fluency in creating programs to solve security problems
- Demonstrate understanding of adversarial thinking, vulnerabilities, and developing defensive strategies
- Demonstrate advanced knowledge of a selected area within the computing security discipline
- Assess the ethical considerations that arise in the computing security field
- Work effectively in teams to accomplish a goal

7. Course Structure:

This course will, primarily, be a lecture-driven course and will focus on Windows systems over Linux or Mac systems.

Many of the lectures will be focused on practical demonstrations rather than traditional PowerPoint slide decks and lectures will be reinforced by requirements attached to the course project. Many aspects of the course projects will require developing small, proof-of-concept features that would be of use in an adversarial simulation. **You should expect to be constantly programming in this course**. Along with programming skills, a base-level understanding of cryptography and exploit development is needed.

The course projects will be group based and peer evaluations will factor heavily into group grades.

8. Tentative Course Outline:

Week	Day 1	Day 2	CSEC 659 Readings
1	Introduction	Legal authorities in Cyber Ops	Cyber Ops & International Relations
2	ATT&CK and Adversary Emulation		Case Study: Equation Group
3	Windows API		Case Study: Operation Aurora
4	Basic Implant Techniques		Case Study: Georgian Invasion
5	PE File Formats		Case Study: DigiNotor
6	Process Injection		Case Study: Pegasus Malware
7	Other Persistence Techniques		Case Study: Saudi Aramco
8	Common C2 Frameworks		Case Study: Sony & The Interview

9	Cobalt Strike	Utility of Threat Intelligence
10	Operational Security for Red Teams	Case Study: Vermillion Strike
11	DevOps for Red Teams	Case Study: Grizzly Steppe
12	Access Operations / Credentialed Access	Case Study: NSO Group & iPhones
13	SEH & Heap Sprays	Case Study: iPhone Baseband Exploit
14	Data Execution Prevention & Bypasses	Vulnerability Equities Processes & Decision Making
15	ASLR and ROP Chains	Case Study: Dark Matter and Project Raven

9. Course Projects Overview:

Threat Actor Profile	• Identify a sector (defense, healthcare, energy, etc) • Identify a threat actor / group actively targeting that sector • Identify key TTP of the threat actor / group to emulate

Implant Project	• Develop a custom malware implant that…
	  o Provides code execution capabilities
	  o Uses the Windows API to provide 2 other payload capabilities
	  o Evades 2 commercial AV platforms
	  o Implements 2 persistence mechanisms

C2 Project	• Build a custom C2 framework that…
	  o Extends your implant to permit remote code execution
	  o Encrypts communications
	  o Employs a covert communication mechanism
	  o Can be deployed in a docker container to cloud infrastructure (AWS EC2, Azure, etc) automatically.

RCE Project	• Develop Powershell to deploy the implant • Develop an Ansible playbook to deploy the implant • Rework two existing remote code execution exploits to deploy the implant

10. Grading:

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

Component	Percentage (CSEC 559)	Percentage (CSEC 659)
PROJECTS/CTQs	**70%**	**70%**
Threat Actor Proj.	17.5%	14%
Implant	17.5%	14%
C2 Framework	17.5%	14%
Exploit	17.5%	14%
Crit. Thinking Qs	--------	14%
Exams (MT/F)	**30%**	**30%** Will have different exams

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

9. Exams, Projects, and Labs/Assignments:

All exams must be taken on the day(s) specified. All projects and lab assignments are due on the date listed in the hand-out provided by the instructor. Exceptions will be made at the sole discretion of the instructor. Some valid reasons may include:

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.

11. Class Attendance

All students are expected to participate in this course for the entire duration of the semester. "Attending class" is recommended, although it may take different forms because of the COVID-19 pandemic. It is my intention to stream all lecture content via Zoom for this course, allowing students to participate even if they cannot attend in-person.

At the time of writing this syllabus, it is unclear if I'll be able to record these streamed lectures and distribute them via MyCourses.

You should not physically attend class if you are feeling sick and you do not need to ask my permission to attend via Zoom instead of in person. There are a host of valid reasons, ranging from transportation challenges to mental health, why a student may choose not to attend CSEC 467 in person. This course will move at a rapid pace, however, and it is your responsibility to ensure that you are continuing to actively participate.

12. Academic Honesty

The following statement is the Policy on Academic Dishonesty for the Computing Security Department.

The Computing Security Department (CSEC) does not condone any form of academic dishonesty. Any act of improperly representing another person's work as one's own (or allowing someone else to represent your work as their own) is construed as an act of academic dishonesty. These acts include, but are not limited to, plagiarism in any form or use of information and materials not authorized by the instructor during an examination or for any assignment.

If a faculty member judges a student to be guilty of any form of academic dishonesty, the student will receive a failing grade for the course. Academic dishonesty involving the abuse of RIT computing facilities may result in the pursuit of more severe action.

If the student believes the action by the instructor to be incorrect or the penalty too severe, the faculty member will arrange to meet jointly with the student and with the faculty member's immediate supervisor. If the matter cannot be resolved at this level, an appeal may be made to the Academic Conduct Committee of the college in which the course is offered.

If the faculty member or the faculty member's immediate supervisor feels that the alleged misconduct warrants more severe action than failure in the course, the case may be referred to the Academic Conduct Committee. The Academic Conduct Committee can recommend further action to the dean of the college including academic suspension or dismissal from the Institute.

The following definitions will be used to clarify and explain unacceptable conduct.
This is not intended to be an exhaustive list of specific actions but a reasonable description to guide one's actions.

CHEATING includes knowingly using, buying, stealing, transporting or soliciting in whole or part the contents of an administered/un-administered test, test key, homework solution, paper, project, software project or computer program, or any other assignment.
It also includes using, accessing, altering, or gaining entry to information held in a computer account or disk owned by another.

COLLUSION means the unauthorized collaboration with another person in preparing written work or computer work (including electronic media) offered for credit. Final work submitted by a student must be substantially the work of that student. Collaboration on an assignment is expressly forbidden unless it is explicitly designated as a group project. When there is any doubt, a student should consult the instructor (NOT ANOTHER STUDENT) as to whether some action Is considered collusion.

Whenever there is any question as to whether a particular action is considered academic dishonesty, the instructor should be consulted PRIOR to commencing that action.

13. Responsible Disclosure

During the course of the semester, students in CSEC 559/659 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, in consultation with the instructor. 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.

14. Course Success

Success in this course depends heavily on your personal health and wellbeing. Recognize that stress is an expected part of the college experience, and it often can be compounded by unexpected setbacks or life changes outside the classroom. Moreover, those with marginalized identities may be faced with additional social stressors. Your other instructors and I strongly encourage you to reframe challenges as an unavoidable pathway to success. Reflect on your role in taking care of yourself throughout the term, before the demands of exams and projects reach their peak. Please feel free to reach out to me about any difficulty you may be having that may impact your performance in this course as soon as it occurs and before it becomes unmanageable. In addition to your academic advisor, I strongly encourage you to contact the many other support services on campus that stand ready to assist you.

15. COVID-19, Year 3 Addendum

Please be advised that, under emergency circumstances, I may be required to alter course requirements, assignment deadlines, attendance expectations, and grading procedures. Please also be advised that the university may have to alter the academic calendar in response to a university. This addendum added as the result of a recommendation in a mass email sent from Dr. Ellen Granberg's office titled "Continuity of Instruction".