

DePaul University CDM

CNS 489 Course Syllabus

Part 1. Instructor and Section Information

Instructor's Name: Ryan Haley

Office Hours: Wednesday 5:00 – 5:45pm, 9:00 – 9:45pm (CDM 342)

Phone: N/A E-mail: rhaley@depaul.edu

Expect responses within 24 hours. Otherwise, reach out again.

Semester: Fall 2017 Section Number: 701 Room Number: CDM 658

Days and hours this section meets: Tuesdays, 6:00pm – 9:40pm

First day of class: Wednesday, September 6, 2017

Last day of class: Wednesday, December 15, 2017

Date of final exam: Wednesday, December 8, 2017

Last Date to Drop and Receive Refund: September 19, 2017

Last Date to Drop this class with a "W" grade: November 8, 2017

Part 2. Course Information

I. Course Identification

Prefix and Number CNS 489

Course Title Cyber Defense Exercises and Attack Responses

Hours

4 Credit Hours

II. Catalog Description

Prerequisite CNS-378 or CSC 374

Corequisite None

Course Description

This is a hands on, laboratory based applied security course in which students will, in teams, defend against cyber attacks and implement services in a hostile cyber environment. Most activities will be derived from Cyber Defense and cyber league competitions and will prepare students to participate and excel in these competitions. This course is open to all students, including inexperienced ones in Cyber Defense competitions. Repeat enrollment is encouraged.

III. Major Course Concepts

- Web Application Security
- Thread Detection
- Log Analysis
- Incident Response
- Protocol Analysis
- Systems Administration and Engineering

IV. Expected Outcomes for Student Learning

1. Students will be able to analyze data for abnormalities and common attack patterns.
2. Students will be able to research systems for known vulnerabilities and perform a risk assessment based on their findings.
3. Students will be able to recognize common weaknesses in everyday services.
4. Students will be able to perform an incident response assessment of a compromised host.
5. Students will be able to analyze network requirements and create advanced firewall rules.
6. Students will learn basic web application security, common vulnerabilities, and how to prevent them.

V. Instructor Policies

- All assignments have a due date. Late assignments will NOT be accepted.
- Students are expected to be on time and attend all in-class sessions.
- Students are expected to always be courteous of others.
- Students are expected to be prepared and participate in class discussions and labs.
- Students are expected to be focused and paying attention during lecture.
- Students are expected to work well with others during group labs and activities.
- Students are expected to complete all labs, online activities and miscellaneous assignments by the due dates.
- The topical outline is solely at the discretion of the instructor and may be modified at any time to better accommodate class time and schedule.
- **Cheating/Plagiarism Policy: Any student caught cheating or plagiarizing will receive zero points for that topic or fail class based on Code of Student conduct rules.**
- Each student is responsible for adhering to the Code of Student Conduct as stated in the college catalog.
- All grades are final. No extra credit will be given.

If students are lacking in any of the above mentioned expectations student's grade may be lowered by one grade level.

VI. Course Websites

- D2L will be used as the main interface for the class. Notes, assignments, and all other course material will be posted here. You can access it by going to d2l.depaul.edu.

Part 3. Classroom Information

I. Topical Outline/Course Schedule/Calendar

(Major course components, assignments, and assessments in a suggested sequence)

<u>Lesson</u>	<u>Date</u>	<u>Topic</u>	<u>Activities Due</u>
<u>1</u>	9/6	Web Basics	
<u>2</u>	9/13	Vulnerability Research	Web Homework 1
<u>3</u>	9/20	Defense Lab Introduction*	Vulnerability Research Homework
<u>4</u>	9/27	Network/Firewall(Network and Host)/Wireshark	NCL Registration ENDS
<u>5</u>	10/4	Offensive Security/Persistence	Network/Firewall Homework
<u>6</u>	10/11	Log Analysis/System Analysis	Offensive Security Homework
<u>7</u>	10/18	System/Services (Email, Web, DNS)	Log Analysis Homework
<u>8</u>	10/25	Web Security	Systems Homework NCL Preseason Game
<u>9</u>	11/1	Incident Response	Web Homework 2 NCL Regular Season Game
<u>10</u>	11/8	Final	Prep for Final
<u>11</u>	11/15	Inject Review/Debrief	IR Homework

II. Books, Supplies, and Supplementary Materials

a. *Textbooks/Reading list*

Required

1. None

Optional

1. *Web Application Hackers Handbook (ISBN: 978-1118026472)*
2. *Blue Team Field Manual (ISBN: 978-1541016361)*

III. Classroom Policies and Procedures

a. *General Information*

b. *College Statement about grades of 'F' and withdrawal from class.*

A student who does not withdraw officially from a course may receive a grade of 'F', depending on course progress or course attendance, which will become a part of the student's permanent record. The withdrawal date is listed in the General Information sheet.

c. *Final Exam Information*

The final exam will be tentatively be given on the 2nd to last day of class.

d. *Attendance Policy*

Attendance is expected but not required. It is the student's responsibility to find out any information that was missed in case of an absence. **Not all required material is documented in lecture notes and examples, and important information will be conveyed verbally during lecture.** If you are falling behind in the class, instructors have the authority to assign points to student's attendance and participation. Excessive absence can affect final grade.

e. *Academic Integrity and Plagiarism*

Cheating and plagiarism is not allowed in this class. Any student caught in the act of cheating/plagiarism will be penalized based on the severity of the offence up to and including immediate dismissal from class and may result in a grade of 'F' in the course.

This is defined as copying another's work and using it as your own. You are free to get ideas from other sources (books, internet, etc), but you are by no means authorized to copy their work and you must cite the original sources from which your ideas stem med.

f. *College Documentation Styles*

MLA and APA have been adopted as the official documentation styles of the college. The selected documentation style for this class is MLA.

g. *Code of Student Conduct*

Each student is responsible for adhering to the Code of Student Conduct as stated in the college catalog.

h. *Cautionary Statement*

Students with an impaired ability to concentrate may risk jeopardizing safety in the classroom for themselves, their classmates and their instructor. If your ability to concentrate is impaired, you should discuss this matter with your instructor prior to operating equipment or performing a laboratory procedure. Students are responsible for reporting to their instructor any condition that would impair the ability to concentrate. Failure to notify your instructor of this issue may be a violation of the Code of Student Conduct.

i. *Safety or Health issues*

Please inform the instructor of any safety concerns or health issues that may affect your learning ability in this class.

j. *Notice of Copyright*

Materials in this course—unless otherwise indicated—are protected by United States copyright law [Title 17, U.S. Code]. Materials are presented in an educational context for personal use and study and should not be shared, distributed, or sold in print—or digitally—outside the course without permission. As a student your ability to post or link to copyrighted material is also governed by United States copyright law. The law allows for students to post or link to copyrighted materials within the course environment when the materials are pertinent to course work. Instructors—or other staff of the institution—reserve the right to delete or disable your post or link if in their judgment it would involve violation of copyright law.

k. *Attitude*

A professional and academic attitude is expected throughout this course. Measurable examples of non-academic or unprofessional attitude include but are not limited to: talking to others

when the instructor is speaking, mocking another's opinion, cell phones ringing, emailing, texting or using the internet whether on a phone or computer. If any issues arise a student may be asked to leave the classroom. The professor will work with the Dean of Students Office to navigate such student issues.

I: Civil Discourse

DePaul University is a community that thrives on open discourse that challenges students, both intellectually and personally, to be Socially Responsible Leaders. It is the expectation that all dialogue in this course is civil and respectful of the dignity of each student. Any instances of disrespect or hostility can jeopardize a student's ability to be successful in the course. The professor will partner with the Dean of Students Office to assist in managing such issues.

m: Incomplete

Incompletes will only be given under extraordinary circumstances. If the student fails to show an acceptable level of work leading up the request, it may be denied by the instructor. If the student is experiencing difficulty during the class, they must reach out before the request is made.

IV. Graded assignments and policies

- a. Homework 40 points
Homework will consist of research problems as well as labs. These are due by 5:45pm each Wednesday.
- b. Quizzes 20 points
Quizzes will be given weekly in lieu of a Midterm. The topic will cover the lecture and homework from the week prior. **Quizzes will only be given in class.** The lowest grade will be dropped.
- c. Team Lab Competition Simulation (Final) 20 points
The final will consist of a simulation exercise meant to mimic the Collegiate Cyber Defense Competition. You will be placed into a team of 4 – 6 students and be required to harden and defend a small business network. A red team, will assess your defenses and try to bring down your core services. All the while, you will be given 'inject' or business tasks to complete during this time. Your final grade will consist of 1) service uptime as calculated from an automated scoring engine. 2) Inject completion and professionalism and 3) Red team assessment. Note that if you find red team has successfully accessed your network, you may submit an IR report to negate the red team penalty. Participation is a requirement. Anyone who fails to participate may have their grade dropped one letter level. Grades may also be adjusted based on team feedback via an evaluation after the exercise.
- d. National Cyber League Participation 15 pts
In lieu of a required text, you will participate in the National Cyber League (NCL) capture the flag (CTF) competition. The cost to participate is \$25. You will not be graded on your score, rather your attempt and effort to solve the various challenges. The preseason and Game 1 are both individual competitions, while the Postseason is a group event. You must participate in the preseason and Game 1 if you wish to participate in the postseason.
<https://www.nationalcyberleague.org/>
 - i. Breakdown:
 1. Preseason – Up to 5 pts
 2. Game 1 – Up to 10 pts
 3. Postseason – Up to 5 pts
- e. Injects/Zombies (Miscellaneous as posted)

- f. *General grading policy, including criteria and weighting for final semester grade*

Grading for courses in this program is as follows;

A = 90 – 100 pts

B = 80 – 89 pts

C = 70 – 79 pts

D = 60 – 69 pts

F = <60 pts

- g. Make-up policy
There are no makeup assignments unless otherwise indicated by the instructor of this course.
- h. Extra-credit policy
There are no extra credit assignments unless otherwise indicated by the instructor of this course.
- i. Late-Work policy
Late work will not be accepted. All assignment deadlines are posted in this syllabus. **This will be strictly enforced.**

Fall 2017 – CNS 489-701 Scripting and Security

1. Last date to drop and get a refund: [9/19/2017](#)
2. Last day to drop this class with a ‘W’ grade: [11/08/2017](#)

College Policies

Changes to Syllabus

This syllabus is subject to change as necessary during the quarter. If a change occurs, it will be thoroughly addressed during class, posted under Announcements in D2L and sent via email.

Online Course Evaluations

Evaluations are a way for students to provide valuable feedback regarding their instructor and the course. Detailed feedback will enable the instructor to continuously tailor teaching methods and course content to meet the learning goals of the course and the academic needs of the students. They are a requirement of the course and are key to continue to provide you with the highest quality of teaching. The evaluations are anonymous; the instructor and administration do not track who entered what responses. A program is used to check if the student completed the evaluations, but the evaluation is completely separate from the student’s identity. Since 100% participation is our goal, students are sent

periodic reminders over three weeks. Students do not receive reminders once they complete the evaluation. Students complete the evaluation online in CampusConnect.

Academic Integrity and Plagiarism

This course will be subject to the university's academic integrity policy. More information can be found at <http://academicintegrity.depaul.edu/>. If you have any questions be sure to consult with your professor.

Academic Policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the University Academic Calendar. Information on enrollment, withdrawal, grading and incompletes can be found at: cdm.depaul.edu/enrollment.

Students with Disabilities

Students who feel they may need an accommodation based on the impact of a disability should contact the instructor privately to discuss their specific needs. All discussions will remain confidential.

To ensure that you receive the most appropriate accommodation based on your needs, contact the instructor as early as possible in the quarter (preferably within the first week of class), and make sure that you have contacted the Center for Students with Disabilities (CSD) at: csd@depaul.edu.

Lewis Center 1420, 25 East Jackson Blvd.

Phone number: (312)362-8002

Fax: (312)362-6544

TTY: (773)325.7296

DePaul University CNS – 489

Code of Academic Integrity

The faculty of DePaul University believe that the Code of Academic Integrity is important because of the professional, academic, and ethical requirements that align the departmental curriculum to the expectations of the occupational environment that our students will be entering. Students are expected to complete all course requirements in a way that reflect the values of the Code of Academic Integrity and encourage others to do the same. Adherence to the Code of Academic Integrity will enable students to participate gainfully in a collegiate learning environment with a high degree of professional ethics and standards, thereby empowering them to be successful after leaving DePaul University.

Cheating and plagiarism have a zero-tolerance policy and will result in immediate failure of the course.

Materials in provided in this class should only be used in authorized settings. Under no circumstances will I use the information I learn without express consent from the appropriate authority.

I attest I have read and understand the terms of the syllabus and the code of conduct and agree to adhere to the policies outlined therein and stated above.

NAME (PRINT): _____

SIGNATURE: _____

DATE: _____