CIS 365: OFFENSIVE SECURITY

Class Schedule:	Monday, Tuesday, Wednesday, Thursday 4pm to 4:50pm
Instructor:	Chad Johnson
Office:	SCI B231
Phone:	715-346-2020
Email:	Chad.Johnson@uwsp.edu
Office hours:	Mondays and Thursdays, 2pm to 3:50pm

COURSE DESCRIPTION

Present and apply network penetration techniques such as reconnaissance, vulnerability assessment, exploitation, and related aspects of offensive-focused security.

COURSE OBJECTIVES

- Perform basic penetration testing.

- Locate and execute exploits in applications.

- Reverse engineer code to locate vulnerabilities.

- Provide ethical penetration testing services.

- Produce effective reports of offensive security efforts.

TEXTBOOK

- Gray Hat Hacking: The Ethical Hacker's Handbook, 5th ed. ISBN-13: 978-1260108415 from McGraw-Hill Education

- We will be using open-source texts, posted to Canvas.

LECTURES

- Lecture notes will be posted in Canvas. I make every effort to make my notes available, but I may decline to include them at my discretion.

- Students are strongly encouraged to attend each class and actively participate in class discussions.

- In general, I do not believe in taking attendance. However, class attendance may be taken in any class without notification in advance.

GRADING

- 3 Quizzes: 15% (5% each)
- 4 Labs: 30% (6% each)
- 3 HTB Challenges: 15% (5% each)
- 4 Simulated Pen Tests: 40% (10% each)

Final grades will be assigned according to the following scale:

A: score >= 90	A-: 87 <= score < 90	
B+: 83 <= score < 87	B: 80 <= score < 83	B-: 77 <= score < 80
C+: 73 <= score < 77	C: 70 <= score < 73	C-: 65 <= score < 70
D: 60 <= score < 65		
F: score < 60		

Scale may be adjusted, depending on the overall performance of the class.

ASSIGNMENTS AND DEADLINES

- This course will involve testing your skills in CTF rooms on HacktheBox.eu. UWSP has a team. You will receive an invite from me to join the team by the end of week 1. If you do not receive this email, let me know. Your work in this course must be done through the team to receive any credit for the assignments.
- Quizzes are open note/book, and you can use the Internet to search for answers. Please do not collaborate on them. They are not group assignments. You will have the week to complete the quiz. Two attempts. Questions will be randomly chosen from a bank. Multiple-choice, multi-select, and true/false only. If you miss a quiz, it cannot be made up.
- The simulated pen test assignments are intended to be followed as closely to a real-world pen-test as possible. That means you must follow the rules and conduct yourself as a professional. You should produce a report that would be aimed at non-security IT and executives, being detailed and with solid recommendations.

OFFICE HOURS POLICY

- I prefer that you contact me via email.

- However, you are still welcome to my office to ask me any questions at any other times.
- I fear the phone.
- Virtual office hours will be posted to Canvas or you can just make an appointment with me through Bookings.

REGRADING

Grades will be posted in Canvas. After the scores are announced, you have 7 days to request regrading by contacting the instructor (office hours or email). Your grade will be final after 7 days.

ACADEMIC INTEGRITY

The university cannot and will not tolerate any form of academic dishonesty by its students. This includes, but is not limited to cheating on examinations, plagiarism, or collusion. **Any form of academic dishonesty may lead to F grade for this course.**

STUDENTS WITH DISABILITIES

If you require accommodation based on disability, please let me know. I am willing to provide any reasonable accommodations you require. The sooner you inform me the better.

FACE COVERINGS

At all UW-Stevens Point campus locations, the wearing of face coverings is mandatory in all buildings, including classrooms, laboratories, studios, and other instructional spaces. Any student with a condition that impacts their use of a face covering should contact the [Disability and Assistive Technology Center](#) to discuss accommodations in classes. Please note that unless everyone is wearing a face covering, in-person classes cannot take place. This is university policy and not up to the discretion of individual instructors. Failure to adhere to this requirement could result in formal withdrawal from the course.

OTHER GUIDANCE

Please monitor your own health each day using [this screening tool](#). If you are not feeling well or believe you have been exposed to COVID-19, do not come to class; email your instructor and contact Student Health Service (715-346-4646).

Note: Schedule / Syllabus is tentative and subject to change.

Note: Schedule / Syllabus is tentative and subject to change.

As with any type of absence, students are expected to communicate their need to be absent and complete the course requirements as outlined in the syllabus.

Maintain a minimum of 6 feet of physical distance from others whenever possible.

Do not congregate in groups before or after class; stagger your arrival and departure from the classroom, lab, or meeting room.

Wash your hands or use appropriate hand sanitizer regularly and avoid touching your face.

Please maintain these same healthy practices outside the classroom.

TENTATIVE SCHEDULE

Week	Lecture Topics	Due	Read
1	Introduction & Syllabus		Ch 1
2	Penetration and Professionalism	Lab 1	Ch 6
3	Bug Bounties and Work Products	Lab 2	Ch 8/9
4	Passive Discovery and Footprinting	Quiz 1	Canvas
5	Locating Vulnerabilities	Pen Test 1	Canvas
6	Cracking Passwords	HTB 1	Ch 10
7	Patch Exploits and Diffing	Quiz 2	Ch 17
8	Malicious Files	Lab 3	Canvas
9	Reverse Engineering	Pen Test 2	Ch 2
10	Binary Exploitation	HTB 2	Ch 4
11	Windows Exploits	Quiz 3	Ch 13/14
12	Web App Penetration	Pen Test 3	Ch 16
13	Fuzzing		Ch 3
14	Injection	HTB 3	Canvas
15	XSS	Lab 4	Canvas
16	Finals Week	Pen Test 4	