

CpS 255
Penetration Testing & Ethical Hacking
Fall 2024

Instructor: Jordan Jueckstock
Office: AL 76 (*third floor, left hall*)
Office Hours: 10:00 – 10:50am daily
Email: jpjuecks@bju.edu

Course Description:

Introduction to the offensive hacking area of penetration testing. Students will demonstrate their understanding of the penetration process (Planning, Reconnaissance, Exploitation, Clean-up & Reporting) through lab exercises.

Course Context:

The material and activities in this course contribute particularly to student progress toward the following Cybersecurity program learning outcomes:

- Cy1: Apply introductory cybersecurity principles to both policy and practice
- Cy4: Communicate technical information effectively, including risks discovered and mitigation strategies
- Cy5: Apply biblical principles of ethics in computing

Course Reading(s):

In lieu of a traditional textbook, we will use open-access resources, including but not limited to technical documentation, research publications, and recorded interviews/documentaries.

Learning Objectives:

By the end of the semester, students will be able to

1. Accurately and simply describe the technical, ethical, and legal bounds of offensive security operations (a.k.a. “penetration testing”, “ethical hacking” or “white-hat hacking”)
2. Explain and summarize the process of vulnerability discovery and exploitation for both technical and semi-technical audiences
3. Demonstrate proficiency at finding and exploiting representative vulnerabilities across a range of designated target systems working both alone and on a team.

Course Schedule:

A provisional (i.e., subject to change) schedule of planned class topics, activities, and due dates is maintained on the course web page: <https://protect.bju.edu/cps/courses/cps255/schedule/>.

Assignments & Grading:

There will be two written tests (including the final exam) covering discussions of definitions, ethics, and vulnerability analysis, as well as a dozen reading quizzes. The primary form of assessment in this class will be technical labs and hacking *challenges* in which students demonstrate proficiency with the tools and techniques discussed in class. *Personal* challenges (PCs) are to be solved and submitted working alone, while the capstone *team* challenge (TC) is to be solved and submitted by a group of students working together. Students must complete the work required by *Labs* themselves but may discuss their solutions freely among themselves.

Grades are computed on a simple 10-point scale (see below) based on points earned out of 1000. Grades are not rounded up (or down—which probably should go without saying). Instead, all students are allotted 5 bonus “grace points” (which have the effect of rounding up, e.g., 695 to 700). The instructor reserves the right to confiscate these grace points, at his sole discretion and at any time, for repeated (or egregious) displays of disrespect to either the instructor or fellow students. (*Students who lose their grace points will be informed as soon as possible.*)

Grading			
#	Item	Pts.	Total
12*	Reading Quiz	5	50
12**	Technical Lab	20	200
3	Personal Challenge	100	300
1	Team Challenge	250	250
2	Written Exam	100	200
-	“Grace points”	5	0
	TOTAL		1000

Scale	
A	900+
B	800-899
C	700-799
D	600-699
F	0-599

*: lowest two (2) quiz grades are dropped

** : lowest two (2) lab grades are dropped

Course Policies:

- *Attendance:* Absence/tardiness is reported per University policy, period.
- *Department:* Compliance with student handbook policies is expected during class. Students and instructor will address each other with professional respect and courtesy, no matter how much fun we are (or are not) having. Students shall refrain from talking (or whispering, or texting, or tapping messages in Morse code, or...) during lectures, presentations, etc. unless otherwise indicated by the instructor.
- *Technology:* personal computers (which, let’s be honest here, includes phones and smart watches) will not be used in class unless called for by the instructor (e.g., during lab sessions). Phones, smart watches, and other communication doodads should be kept silent and passive except for high-priority communications previously discussed with the instructor (e.g., waiting for word about a sick family member).
- *Due dates:* See the department late policy <https://cs.bju.edu/academics/policies/late-work-policy/>. A “free late” is (a) earned by prior demonstration of responsible, competent work, (b) negotiated with the instructor before the due date in question, and (c) not applicable for any group work.
- *Academic Integrity:* See the department cheating policy: <https://cs.bju.edu/academics/policies/academic-integrity-policy/>. The technical artifacts produced for each personal challenge should be treated as *individual program code* per the policy and should never be shared in any way between students. Students *may* discuss how to approach a given challenge in general terms, and alert each other to time-consuming dead-ends, but students must make a *bona fide* effort not to “give away” solutions (or essential “plot spoilers” that lead directly to solutions).
- *Generative AI:* Students are allowed the use of generative AI tools to (a) research and understand technical evidence gathered from target systems and (b) craft scripts or other attack tools for use against authorized targets. No other use (e.g., generating text for a report or other written assignment) is permitted. Students using generative AI tools (a) *must* disclose this fact prominently in their report or submission comments, (b) *must* include a substantive written assessment of how the tool’s output helped (or did not), and (c) *must* provide full transcripts of their AI tool interactions (prompts entered, artifacts generated) along with their other submission artifacts.

Copyright Policy:

Copyright 2023-2024 Jordan Jueckstock as to this syllabus and all lectures. Students are prohibited from selling (or being paid for taking) notes during the course to, or by any person, or commercial firm without the express written permission of the professor teaching the course.