​​​​​​​​​​**CpS 392 – Cyber Operations**

Spring 2025

|  |  |  |
| --- | --- | --- |
| C:\Users\ahughes\Desktop\Dr. Alan Hughes.jpg​Instructor: Dr. Alan Hughes | **Instructor:** | Dr. Alan Hughes |
| **Office:** | AL76Alternatively, CS Lab (Mack Library, 2nd floor, MB203) |
| **Office Hours:** | MWThF 10am by appointment; Tue. Electronic by appointment​ |
| **Email:** | ahughes@bju.edu |
| **Telephone:** | Cell: 864-906-1024Office: 86-242-4100 x​2274​ |

**Course Description:**

Develops hands-on training and processes to build, attack, and defend computer networks and servers, includes both offensive and defensive techniques addressing networks, virtual testing, and web applications/servers/databases. Consideration will be given to designing a defensive infrastructure, including firewalls, logging, and intrusion detection/prevention systems and an introduction to white hat hacking.

**Course Reading(s):**

CompTIA CySA+ Guide to Cybersecurity Analysis, 3rd Edition, COPYRIGHT © 2025 Cengage Learning, Inc., ISBN: 979-8-214-01147-9

****

**Context:**

The faculty of the Computer Science department has aligned the computer science program with the goals of the Mathematical Sciences Division, the BJU Bible and liberal arts core objectives, and the BJU institutional goals. The goal of the Computer Science department is to align all courses in the Computer Science and Information Technology majors to support one or more of the following departmental goals. An asterisk indicates a specific goal fulfilled by this course.

1. Design and implement solutions to practical problems. \*
2. Demonstrate an ability to work effectively in teams. \*
3. Demonstrate an ability to communicate technological information effectively both in written and oral forms. \*
4. Demonstrate an ability to acquire new knowledge in the computing discipline. \*
5. Demonstrate an understanding of social, professional and ethical considerations related to computing. \*
6. Demonstrate understanding of fundamental concepts in the discipline. \*
7. Prepare students for graduate school or to secure employment in a related area. \*

**Course Goals:**

1. Design and implement solutions to practical problems.
2. Demonstrate an ability to work effectively in teams.
3. Demonstrate an ability to communicate technological information effectively both in written and oral forms.
4. Demonstrate an ability to acquire new knowledge in the computing discipline.
5. Demonstrate understanding of fundamental concepts in the student's discipline.
6. Provide the student a platform for continued learning and development of his God-given abilities.
7. Instill in the student a desire to use his abilities in service to Christ.

**Learning Objectives:**

At the end of the course, students should be able to:​

|  |  |
| --- | --- |
| **Learning Objectiv​es** | **Assessment Tools​** |
| 1. Understand how to install various operating systems as virtual machines, using current virtualization technologies. | Lab Assignments, Lab Tests |
| 2. Understand the common attacks on hosts, servers, and computer networks, and the methods used to conduct and detect those attacks. | Lab Assignments, Lab Tests |
| 3. Understand the how to construct a defense against common host, server, and network attacks. | Lab Assignments, Lab Tests |
| 4. Understand the ethical considerations of modern cyber operations and cyber warfare. | Writing Assignment |

​​

**Course Policies:**

**Qualifications**

CpS 335 is a pre-requisite course for CpS 392.

**Absences, lateness, and makeup opportunities**

1. The overarching guide for class attendance is the [BJU Class Attendance Policy](http://home.bju.edu/life/policies/class-attendance-policy.php).
2. For planned absences, please email me one week in advance.
3. Written assignments should be submitted before your planned absence.
4. Scheduled tests and quizzes should be taken before your planned absence; please contact me to make arrangements for doing so.
5. For absences due to incapacitating illness or emergency, you should contact me as soon as you are able to return to class in order to make arrangements for making up any graded work without penalty.
6. In other circumstances, tests and quizzes may be made up within one week of your return, with a 10 percent grade penalty for that test or quiz.
7. Leaving class early without prior arrangement will constitute an absence.

**Late Work**

1. Assignments must be submitted using the electronic submission system before midnight on the day due.
2. The use of the submission system will be explained during the first week of class.
3. Only work missed for legitimate reasons may be made up without penalty. Legitimate reasons include illness, a death in the family, or a BJU sanctioned tour.
4. You must make up late work according to the number of days missed - that is, missing one day of class gives you one extra day to turn in your work.
5. Any other late work will receive a 25% grade penalty.
6. All late work must be made up within one week in order to receive a non-zero grade.

**Grade appeals**

1. Grading appeals must be made by email only no later than one week after the grade was assigned.
2. Appeals will be automatically denied if the student attempts to make the appeal verbally.
3. Email grading appeals should be made respectfully and logically ("My grade should be increased because.....").

**Academic Integrity**

1. The overarching guide for academic integrity is the [BJU Academic Integrity Policy](http://home.bju.edu/academics/integrity.pdf).
2. Cheating on assignments and tests is a form of deception and stealing, and as such, is prohibited by Scripture and will incur academic penalties.
3. All work is to be done individually unless Dr. Hughes gives permission for group work.
4. In general students are encouraged to assist one another in the lab environment *but must exercise care when seeking assistance while completing labs*.
5. Since the goal of the assignments in this course is to learn to develop the skills covered NOT complete the tasks assigned, and since the use of AI to complete or jumpstart tasks defeats the goal of the assignments, you may not use generative AI tools (i.e. Chat GPT, Bing Chat, Google Bard, etc.) in this course for any assignment without the professor’s express permission.  Should an AI tool be used with permission, its use must be documented.
6. **The goal is for each student to become familiar with information security and secure operations and be able to work effectively on his or her own. Therefore, please do not copy work from another person, as this constitutes cheating. This includes using material from Internet or other sites without attribution.**

**Class Participation**

1. Compliance with student handbook policies, including the dress code, is expected during class.
2. Class participation grades are based upon actively participating in lecture class discussions, working diligently on course assignments in lab classes and being respectful to the rest of the class and the instructor.
3. Class participation grade will include in-class assignments throughout the semester that will be individually graded.
4. Playing games, electronic messages, working on other subjects, etc. is a demonstration of disrespect for both the instructor and other students, and is not allowed during lecture and lab classes.
5. Earbuds of any kind may not be worn in class.
6. Professional dress required for any presentations.
7. Violations of this policy may result in a recorded absence for that class period.

**Instructor Help Outside of Class**

You are encouraged to use **email** or the telephone to ask Dr. Hughes for assistance.

**Copyright Policy**

Copyright 2019-2025, Alan Hughes, 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.​

**Schedule** (may be modified as needed during semester)

**Note: Quiz dates are in Canvas**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date**  | **Day**  | **Class**  | **Assignment** **Due** |
| **Week 1** |  | **Technology Underpinnings** |  |
| Jan 16 | Th | Introduction; Syllabus | **Read Chapter 1** |
| **Week 2** |  | **Threats Actors and Their Threats** |  |
| Jan 21 | T |  | **Read Chapter 2** |
| Jan 23 | Th |  | **Lab 1** |
| **Week 3** |  | **Cybersecurity Substrata** |  |
| Jan 28 | T |  | **Read Chapter 3** |
| Jan 30 | Th |  | **Lab 2** |
| **Week 4** |  | **Identifying Indicators of Attack** |  |
| Feb 4 | T |  | **Read Chapter 4** |
| Feb 6 |  Th |  | **Lab 3** |
| **Week 5** |  | **Analyzing Indicators of Compromise** |  |
| Feb 11 | T |  | **Read Chapter 5** |
| Feb 13 | Th |  | **Lab 4** |
| **Week 6** |  | Bible Conference |  |
| Feb 18 | T | **Test 1 – Ch 1-5** |  |
| Feb 19-21 |  | **Bible Conference** |  |
| **Week 7** |  | **Threat Detection and Process Improvement** |  |
| Feb 25 | T |  | **Read Chapter 6** |
| Feb 27 | Th |  | **Lab 5** |
| **Week 8** |  | **Vulnerability Scanning and Assessment Tools** |  |
| Mar 4 | T |  | **Read Chapter 7** |
| Mar 6 | Th |  | **Lab 6** |
| **Week 9** |  | **Addressing Vulnerabilities** |  |
| Mar 11 | T |  | **Read Chapter 8** |
| Mar 13 | Th |  | **Lab 7** |
| **Week 10** |  | **Vulnerability Management and Administration** |  |
| Mar 18 | T |  | **Read Chapter 9** |
| Mar 20 | Th |  | **Lab 8** |
| **Week 11** |  | Spring Break! |  |
| **Week 12** |  | **Incident Response and Planning** |  |
| Apr 1 | T |  | **Read Chapter 10** |
| Apr 3 | Th |  | **Lab 9** |
| **Week 13** |  | **Incident Response and Activity Phases** |  |
| Apr 8 | T |  | **Read Chapter 11** |
| Apr 10 | Th |  | **Lab 10** |
| **Week 14** |  | **Data Protection and Utilization** |  |
| Apr 15 | T |  | **Read Chapter 12** |
| Apr 17 | Th |  | **Lab 11** |
| **Week 15** |  | **Test 2; Biblical Ethics of Security** |  |
| Apr 22 | T | Test 2 |  |
| Apr 24 | Th | Biblical Ethics of Security | **Lab 12** |
| **Week 16** |  | **Hands-on Cyber Attacks** |  |
| Apr 29 | T | Prepare |  |
| May 1 | Th | Attack/Defend |  |
| **Exam Week** |  |  |  |
| May 6 | T | **2-3:10pm- Final Exam****Note:** If you pass the CompTIA [CySA+ certification exam](https://www.comptia.org/certifications/cybersecurity-analyst) before the final you are exempt from taking it (given that you have done all the other required work for the course with good quality (B- or better)). |  |

**Grading​**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Item** | **Pts.** | **Total** |
| 12 | Labs | 35 | 420 |
| 12 | Quizzes | 25 | 300 |
| 1 | Paper: Biblical Ethics of Cybersecurity | 100 | 100 |
| 1 | Final Exam | 100 | 100 |
| 1 | Class Participation | 100 | 100 |
| ​ | **TOTAL** | ​ | 1020 |

**Grading Scale**

|  |  |
| --- | --- |
| A | 90-100 |
| B | 80-89 |
| C | 70-79 |
| D | 60-69 |
| F | < 60​​ |

