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

Spring 2020

**Notice:** For the remainder of the Spring 2020 semester, Canvas will be the schedule of record. Tests will be open-book, including the final exam (if we have one). For classes with presentations, you (and your teammates) will separately record your portion, and then edit them together into one presentation. Don’t panic, you can do it. Nothing will be due from March 16-Mar 30, but on Mar 31 things will start being due. All due dates as of April 6 will remain in place, with some adjustments possible during the last week of April, due to final grade reporting requirements. I will be in my office.

For labs using routers and switches, you can use virtual software like GNS3 (version 0.8.3 is best and easiest). IOSs are in the course content, or you can find them online. Alternatively, you can use another virtual network design tool, and use either Juniper or Cisco emulation. You are all smart, and can figure this out. If you can figure out the video games that you manage to overcome, you can do this…. ☺

Keep up with the Canvas schedule – do not get behind! Easier to keep up than to catch up. We will all finish this together.

|  |  |  |
| --- | --- | --- |
| C:\Users\ahughes\Desktop\Dr. Alan Hughes.jpg  ​Instructor: Dr. Alan Hughes | **Instructor:** | Dr. Alan Hughes |
| **Office:** | AL76  Alternatively, CS Lab (Mack Library, 2nd floor) |
| **Office Hours:** | MWF 2pm; Th 10am; Tue electronic​ |
| **Email:** | [ahughes@bju.edu](mailto:ahughes@bju.edu) |
| **Telephone:** | Cell: 864-906-1024  Office: 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):**

Cyber Operations: Building, Defending, and Attacking Modern Computer Networks, Mike O’Leary, 2nd Edition. ISBN: 978-1-4842-4293-3

Other readings as assigned.

**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 20% 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. **The goal is for each student to become familiar with information security, 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. Professional dress required for any presentations.

**Instructor Help outside of class**

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

**Copyright Policy**

Copyright 2019-2020, 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)

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Day** | **Class** | **Assignment** **Due** |
| **Week 1** |  |  |  |
| Jan 16 | Th | Introduction and Syllabus; LMS; Introduction to Cyber Operations | Review Syllabus |
| **Week 2** |  | **System Setup** |  |
| Jan 21 | T | VMWare; Building Linux Systems |  |
| Jan 23 | Th | Building Windows Systems (VMs) |  |
| **Week 3** |  | **Basic Offense** | Lab 1 |
| Jan 28 | T | Ethics; Vulnerabilities; Metasploit (Attacking the browser) |  |
| Jan 30 | Th | Metasploit and Meterpreter commands |  |
| **Week 4** |  | **Operational Awareness** | Lab 2 |
| Feb 4 | T | Intro; Linux Tools |  |
| Feb 6 | Th | Windows Tools; Network Tools |  |
| **Week 5** |  | **DNS and BIND** | Lab 3 |
| Feb 11 | T | Installing BIND; Master Config | **Test 1 (take-home)** |
| Feb 13 | Th | Querying DNS; Advanced Config | **Lab Test 1 (take-home)** |
| **Week 6** |  |  | Lab 4 |
| Feb 18-21 |  | **Bible Conference** |  |
| **Week 7** |  | **Scanning the Network/AD** |  |
| Feb 25 | T | Scanning (NMAP and Metasploit) |  |
| Feb 27 | Th | AD/DNS/Running commands remotely |  |
| **Week 8** |  | **Attacking the Domain/Logging** | Lab 5 |
| Mar 3 | T | Windows (Recon, PE, Attacks) |  |
| Mar 5 | Th | Linux Privilege Escalation; Logging |  |
| **Week 9** |  | **Network Services** | Lab 6 |
| Mar 10 | T | SSH; FTP |  |
| Mar 12 | Th | Windows File Sharing; Remote Desktop |  |
| **Week 10** |  | **Malware and Persistence** | Lab 7 |
| Mar 17 | T | Document-based Malware; Malware Analysis | **Test 2 (take-home)** |
| Mar 19 | Th | Persistence; Detecting Persistence | **Lab Test 2 (take-home)** |
| **Week 11** |  |  |  |
| Mar 23-27 | M-F | **Spring Break** |  |
| **Week 12** |  | **Apache, IIS, ModSecurity; Web Attacks** | Lab 8 |
| Mar 31 | T | Apache, IIS, MS |  |
| Apr 2 | Th | Web Attacks |  |
| **Week 13** |  | **Firewalls** | Lab 9 |
| Apr 7 | T | Network Firewalls |  |
| Apr 9 | Th | IPFire; Attacks through firewalls |  |
| **Week 14** |  | **Databases; Snort** | Lab 10 |
| Apr 14 | T | Using and attacking MySQL |  |
| Apr 16 | Th | Snort |  |
| **Week 15** |  | **PHP; Web Applications** | Lab 11 |
| Apr 21 | T | Attacking PHP | **Ethics Paper Due** |
| Apr 23 | Th | BASE; phpMyAdmin |  |
| **Week 16** |  | **More Web Apps** | Lab 12 |
| Apr 28 | T | Joomla; Wordpress |  |
| Apr 30 | Th | ZenCart | **Lab Test 3 (take-home)** |
| **Exam Week** |  |  |  |
| May 4 | 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)). | **Comprehensive** |

**Grading​**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Item** | **Pts.** | **Total** |
| 12 | Labs | 30 | 360 |
| 2 | Lab tests | 100 | 200 |
| 1 | Research Paper | 150 | 150 |
| 1 | Final Exam | 100 | 100 |
| 1 | Class Participation | 100 | 100 |
| ​ | **TOTAL** | ​ | 910 |

**Grading Scale**

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

