

**IDC 5606 Cyber Defense Operations and Incident Response**

FALL 2022 | DAYS TIME-TIME | ROOM MODE OF INSTRUCTION: ONLINE

STUDENTS ALL MEET WITH INSTRUCTOR FOR CLASS SYNCHRONOUSLY, USING A MULTI-MEDIA CONFERENCING SYSTEM SUCH AS

COLLABORATE, AT A SPECIFIC CLASS TIME INDICATED IN THE UNIVERSITY’S COURSE SCHEDULE FOR EACH SEMESTER. ADDITIONAL

ASYNCHRONOUS INTERACTIONS (E.G., DISCUSSION FORUMS) AMONG STUDENTS AND WITH INSTRUCTOR MAY ALSO BE REQUIRED TO COMPLETE THE COURSE.

**Instructor:** Dr. Shuyuan Metcalfe

**Office:** Shores 250

**Office Hours:** By appointment **E-mail:** smho@fsu.edu **Phone:** (850) 645-0406

**Course Website:** https://directory.cci.fsu.edu/shuyuan-metcalfe/

**COURSE PREREQUISITES:** LIS4774/LIS5775 or approved by instructor

## COURSE DESCRIPTION:

This course provides students with practical experience on computer incident handling, diagnostic reporting, incident response, and cyber defense operations. Students will gain experience in forming effective, cohesive and efficient cyber defense teams. Students will be grouped into teams to configure and secure various types of information systems (e.g., Redhat, Debian, Windows, etc.) that provide on-demand services (such as ftp, http, firewall, etc.) within an organizational setting. In particular, students will follow principles of computer incident handling, reporting and response exercises, as well as operational exercises as part of tabletop incident discussions. Industry-based technical and system-based exercises (e.g., Palo Alto Networks, Redhat etc.) will be simulated in a cloud-based lab environment. The course instructional design is semi-structured but highly interactive. Students are required to work with one another in teams to solve operational and technical problems. Students will also have a chance to participate in on-campus, regional and national Collegiate Cyber Defense Competition (CCDC), with an opportunity to advance their critical thinking and troubleshooting skills in a virtual “sandbox,” for solving current cyber threat issues. Students in graduate programs will be expected to have leadership, management and technical problem-solving skills, and be able to articulate the research problems of cyber defense operations and incidents response with theoretical and methodological approaches.

## COURSE OBJECTIVES:

After successful completion of this course, students will be able to:

* Determine why and how to organize an incident response (IR) team
* Articulate key strategies for making the case to senior management
* Assemble and develop the IR team in organizational hierarchy for maximum effectiveness
* Review best practices for managing attack situations with your IR team
* Construct and develop relationships with other teams, organizations, and law enforcement to improve incident response effectiveness
* Plan how to form, organize and operate as a cyber defense team to deal with system vulnerabilities and assess their severity
* Recognize the differences between vulnerabilities and exploits of various information systems and devices
* Employ techniques on how to coordinate all the entitles involved in incident handling
* Administer and implement the steps for handling system vulnerability
* Adapt strategies and best practices for notifying stakeholders about vulnerabilities and ensuring deployable fixes

## COURSE MATERIALS:

There is no required text. Required readings will be posted on the course website.

(Optional) Rajnovic, Damir (2011) Computer Incident Response and Product Security. Cisco Press PTG. ISBN: 978-0132491495.

## COURSE ASSIGNMENTS:

**Individual-based Weekly Lab Exercises** (60%): There are weekly hands-on lab exercises for this class. We will offer industry-based and open source information systems along with product experience for incident handling, reporting and response principles as they are deployed in real life; these labs will give you extensive experience in all of these categories. You must be in the lab to complete these lab exercises. You can work and coordinate with one another as teams, and address system vulnerabilities in your protected networks, but your submitted work must be done individually on your assigned virtual machines. You will log and document the actions for each lab project and submit a final report with procedures and explanations to the designated submission folder on the course website *on or before the due dates listed on the course schedule*.

**In-Class Participation** (5%):: Attendance will be taken throughout the semester. Active in-class participation and interaction with the team members will be part of the weekly assignments. This will be 5% of your total grade for this class.

* + This is an advanced class. *Class contribution* will include both asking and answering questions, discussing homework assignments and cases, as well as sharing material read from outside sources (or from your own experience). Passive observers will lose substantial points. *I will expect you to help identify systems vulnerabilities and troubleshoot technical problems*. Class participation will also be assessed based on your contribution to the team’s coordination activities throughout the semester. Class participation will require common *courtesy*. That means it will be considered inappropriate to be chronically late to class, to talk with other people during lectures, surf the web or answer cell phones during class. Students’ performance will be monitored and recorded.

**Team-based Incident Response** (35%): The projects for this class will be some of the best experiences you will have. The class will be divided into groups of students. These IR projects will give you experiences with addressing computer incident handling and response. You will work with your assigned team members and perform tabletop exercises on core incident scenarios. You will apply incident response, handling and reporting principles instructed in the course as in real life. Moreover, you will have an opportunity to configure virtual machines—both open source as well as industry-based devices—and troubleshoot server vulnerabilities, and penetrate systems within ethical conduct considerations, detecting various types of cybersecurity attacks using advanced security tools.

* + **Weekly Deliverables** (25%): There are ten (10) deliverables consisting of several projects each. Specific deliverables will be announced at the beginning of the class, and before each due date. You will track activities via screenshots for each project and submit a report to the designated submission folder on the course website *on or before the due dates listed on course schedule*.
	+ **Final Project Deliverables** (10%): There is one (1) final project for this course, and the deliverables will consist of technical activities such as penetration testing and cyber defense and protection of your individually assigned virtual machines as well as for each team. The project will have several checkpoints throughout the semester. The final project results will be presented at the end of semester. Specific deliverables will be announced at the beginning of the class, and before each due date. You will track activities via screenshots for each project and submit a report to the designated submission folder on the course website *on or before the due dates listed on course schedule*.

## GRADE CALCULATION:

Course grade will be generally based on a series of weekly lab assignments, technical exercises, term paper, in- class participation, and attendance. More information about group-based project assignments will be provided during class.

All of your submitted assignments for this class must be original. Plagiarism of any type, including copying and pasting material from Internet sources, will not be tolerated. Before submitting any work for this class, please read the "Academic Honor System" in its entirety (see link below) and ask me to clarify any expectations that you do not understand.

More information about exams and assignments will be provided during class.

**Assignments will be weighted as follows:**

|  |  |
| --- | --- |
| Lab/homework assignments | 60% |
| Team-based IR forum (10) | 25% |
| * Problem-solving reports
* IR reports
 |  |
| Team-based IR final project & presentation | 10% |
| Participation | 5% |

|  |  |
| --- | --- |
| **Total** | **100%** |

## GRADING SCALE:

|  |  |  |  |
| --- | --- | --- | --- |
| A | 93 – 100% | C | 73 – 76 |
| A- | 90 – 92 | C- | 70 – 72 |
| B+ | 87 – 89 | D+ | 67 – 69 |
| B | 83 – 86 | D | 63 – 66 |
| B- | 80 – 82 | D- | 60 – 62 |
| C+ | 77 – 79 | F | 0 – 59 |

**COURSE SCHEDULE:**

The class will meet twice a week. We may additionally incorporate hybrid techniques e.g., virtualization, network defense solutions from open source distribution, Palo Alto Networks, Redhat Linux, etc. into our lab exercises. Below is a tentative schedule and is subject to change with advance notice (Please refer to *Syllabus Change Policy*).

|  |  |
| --- | --- |
| **WEEK** | **TOPIC** |
| 1 | Introduction |
| 2 | Why care about incident response? |
| 3 | Forming and operating an IRT |
| 4 | Creating and operating a cyber defense team |
| 5 | Incident coordination in team |
| 6 | Dealing with an attack (1) |
| 7 | Dealing with an attack (2) |
| 8 | Information systems solutions from global vendors |
| 9 | System vulnerabilities & Security vulnerability notification |
| 10 | Security vulnerability handling by vendors |
| 11 | Vulnerability coordination (1) |
| 12 | Vulnerability coordination (2) |
| 13 | Vulnerability coordination (3) |
| 14 | Finalizing term project |
| 15 | Team presentation |

# SCHOOL POLICIES

### Copyright Statement

Some of the materials in this course are possibly copyrighted. They are intended for use only by students registered and enrolled in this course and only for instructional activities associated with, and for the duration

of, the course. They may not be retained in another medium or disseminated further. They are provided in compliance with the provisions of the Technology, Education, And Copyright Harmonization (TEACH) Act (refer to the 3/7/2001 TEACH Act at [www.copyright.gov/legislation/archive/](http://www.copyright.gov/legislation/archive/) ).

### Sexual Harassment Policy

It is the policy of the University that its employees and students neither commit nor condone sexual

harassment in any form. <http://registrar.fsu.edu/bulletin/graduate/information/university_notices/>

### iSchool Hardware and Software Requirements

A list of all hardware and software requirements for students participating in the School of Information (iSchool) courses can be found at the following

location: <http://ischool.cci.fsu.edu/academics/online/requirements/>

### Student Eligibility for an Incomplete Grade

Incomplete (“I”) grades will not be assigned, except in the case of exceptional unforeseen circumstances that occur within the last three weeks of the semester and your work has otherwise been satisfactory.

# UNIVERSITY POLICIES

### University Attendance Policy:

Excused absences include documented illness, deaths in the family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. These absences will be accommodated in a way that does not arbitrarily penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

### Academic Honor Policy:

The Florida State University Academic Honor Policy outlines the University's expectations for the integrity of students' academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process. Students are responsible for reading the Academic Honor Policy and for living up to their pledge to "...be honest and truthful and...[to] strive for personal and institutional integrity at Florida State University." (Florida State University Academic Honor Policy, found at <http://fda.fsu.edu/Academics/Academic-Honor-Policy>)

### Academic Success:

Your academic success is a top priority for Florida State University. University resources to help you succeed include tutoring centers, computer labs, counseling and health services, and services for designated groups, such as veterans and students with disabilities. The following information is not exhaustive, so please check with your advisor or the Dean of Students office to learn more

### Americans With Disabilities Act:

Florida State University (FSU) values diversity and inclusion; we are committed to a climate of mutual respect and full participation. Our goal is to create learning environments that are usable, equitable, inclusive, and welcoming. FSU is committed to providing reasonable accommodations for all persons with disabilities in a manner that is consistent with academic standards of the course while empowering the student to meet integral requirements of the course.

To receive academic accommodations, a student:

1. must register with and provide documentation to the Office of Accessibility Services (OAS);
2. must provide a letter from OAS to the instructor indicating the need for accommodation and what type; and,
3. should communicate with the instructor, as needed, to discuss recommended accommodations. A request for a meeting may be initiated by the student or the instructor.

Please note that instructors are not allowed to provide classroom accommodations to a student until appropriate verification from the Office of Accessibility Services has been provided. This syllabus and other class materials are available in alternative format upon request. For more information about services available to FSU students with disabilities, contact the

### Office of Accessibility Services

874 Traditions Way

108 Student Services Building Florida State University Tallahassee, FL 32306-4167

(850) 644-9566 (voice)

(850) 644-8504 (TDD)

**oas@fsu.edu**[**https://dsst.fsu.edu/oas**](https://dsst.fsu.edu/oas)

### Syllabus Change Policy

"Except for changes that substantially affect implementation of the evaluation (grading) statement, this syllabus is a guide for the course and is subject to change with advance notice."

### Classes Subject to HB233 Recording

In this class, consistent with state law and university policy, students are permitted to make recordings of class lectures for personal use only. As noted, sharing, posting, or publishing classroom recordings may subject you to honor code violations and legal penalties associated with theft of intellectual property and violations of other state law. Moreover, students and educators have expressed concern that recording classroom activities may negatively impact the learning experience for others, especially in classes that involve questions, discussion, or participation. To protect a learning environment in which everyone feels free to experiment with ideas, we ask you refrain from recording in ways that could make others feel reluctant to ask questions, explore new ideas, or otherwise participate in class. Students must monitor their recording so that they do not include participation by other students without permission. Students with disabilities will continue to have appropriate accommodations for recordings as established by the Office of Accessibility Services.

### Confidential campus resources:

Various centers and programs are available to assist students with navigating stressors that might impact academic success. These include the following:

**Victim Advocate Program** University Center A, Rm. 4100 (850) 644-7161

Available 24/7/365 Office Hours: M-F 8-5 <https://dsst.fsu.edu/vap>

### University Counseling Center

Askew Student Life Center, 2nd floor 942 Learning Way

(850) 644-8255

<https://counseling.fsu.edu/>

**University Health Services** Health and Wellness Center (850) 644-6230

<https://uhs.fsu.edu/>