Enterprise Security

Class Periods: Tu 3-350 Period 8 / Th 3-455 Period 8,9

Academic Term: Spring 2021

Instructor:
Cheryl Resch
Cheryl.resch@ufl.edu
Office Hours: M 4pm, Tu 4pm

Course Description

Provides an introduction to the real-world aspects of defending an enterprise network. Students will gain hands-on experience performing system security tasks and handling incidents. The class begins with a basic introduction to enterprise cybersecurity, the attack sequence, and managing cybersecurity. Then lecture, homework and lab activities cover the center for internet security's twenty essential security controls.

Course Pre-Requisites

CDA 3101

Course Objectives

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

- Identify and think critically about weaknesses in an enterprise network
- Assess risk and prioritize problem areas
- Identify controls to mitigate risk

Materials and Supply Fees

none

Required Textbooks and Software

None

Recommended Materials

None

Course Schedule

Week / Topics / 'NICE Challenge' Lab / Assignment

1 / Defining the cybersecurity challenge, Enterprise security frameworks
2 / Risk analysis / 'Radical Risk Reduction' / HW1 Risk analysis
3 / Cybersecurity attack sequence, Security policies / 'Malicious malware' / HW2 Research an attack
4 / Inventory and control of hardware and software / 'Assuring accurate asset inventories' / Discussion 1 - hardware/software inventory products
5 / Continuous vulnerability management / 'Vulnerability scan complete, begin system hardening' / Discussion 2 - vulnerability management products
6 / Access control / 'Secure roots: domain organization and access controls'/HW3 Access control
7 / Secure configurations / 'STIG Solutions'
8 / Auditing / 'Legitimate Logging Logistics'
9 / Email and web browser protections / 'Malicious mail management' / Discussion 3 - email and web browser management products
10 / Boundary defense / 'Firewall update: tables for two' / HW4 - Firewalls
11 / Data protection and recovery / 'Data backup and recovery, definitely worth testing' / Discussion 4 - Data backup and recovery products
12 / Security awareness and training / 'Dangerous drives' / Discussion 5 - Security awareness and training

13 / Account monitoring and control / 'Networking anomalies: Policy Implementation'
14 / Incident Handling / 'Malware aftermath clean up'
15 / Penetration tests and read team exercises / 'Penetration Testing: Bringing passwords up to snuff' / Paper

F2F Course Policy in Response to COVID-19

We will have face-to-face instructional sessions to accomplish the student learning objectives of this course. In response to COVID-19, the following policies and requirements are in place to maintain your learning environment and to enhance the safety of our in-classroom interactions.

- You are required to wear approved face coverings at all times during class and within buildings. Following and enforcing these policies and requirements are all of our responsibility. Failure to do so will lead to a report to the Office of Student Conduct and Conflict Resolution.
- This course has been assigned a physical classroom with enough capacity to maintain physical distancing (6 feet between individuals) requirements. Please utilize designated seats and maintain appropriate spacing between students. Please do not move desks or stations.
- Sanitizing supplies are available in the classroom if you wish to wipe down your desks prior to sitting down and at the end of the class.
- Follow your instructor's guidance on how to enter and exit the classroom. Practice physical distancing to the extent possible when entering and exiting the classroom.
- If you are experiencing COVID-19 symptoms (Click here for guidance from the CDC on symptoms of coronavirus), please use the UF Health screening system and follow the instructions on whether you are able to attend class. Click here for UF Health guidance on what to do if you have been exposed to or are experiencing Covid-19 symptoms.
- Course materials will be provided to you with an excused absence, and you will be given a reasonable amount of time to make up work. Find more information in the university attendance policies.

Attendance Policy, Class Expectations, and Make-Up Policy

Class attendance on Thursdays for NICE challenges in person or via Zoom is required.

Homeworks, discussions, and the paper must be submitted on time unless there is a university approved excuse. Late assignments will receive no credit.
Excused absences must be in compliance with university policies in the Graduate Catalog (http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#attendance) and require appropriate documentation.

Evaluation of Grades

Assignment	Total Points	Percentage of Final Grade
Labs (13, 1 drop)	100 each	50%
Homeworks (5)	40 each	15%
Discussions (6, 1 drop)	10 each	15%
Paper	100	20%
		100%

Labs

Labs are done on Thursdays during the class period via https://nice-challenge.com/. Each student will have access to a virtual environment where they will carry out tasks as specified in the lab. Students will document how they accomplished each tasks. Collaborating with classmates is welcomed and encouraged. Grading is based on completing and documenting the tasks.

Homeworks
Homeworks consist of problems and short answer questions. They are assigned on Tuesdays and due on the following Monday and may not be turned in late.

Discussions
Discussions are conducted through the Canvas Discussion link. Discussions are assigned on Tuesdays and due on the following Monday. This will entail researching and describing an enterprise security tool for a specific need (e.g. vulnerability scanner).
Rubric
On time post, 3-4 sentences describing tool, features and strengths of tool 10 points
On time post, vague or brief (2 sentences or less) description of tool.

Paper
The paper is due on the last day of the semester and may not be turned in late.
Choose an enterprise. Examples are a university, a company, a county government, an office. Design security for this enterprise.
The paper must include:

Title

Introduction - Describe the enterprise. What industry sector is it in? How large is the enterprise? Brief description of operations.

Asset inventory - what are the assets of this enterprise? Which are the most important assets? What is the level of confidentiality, integrity and availability required for each asset?

User groups and access control - Describe user groups. What data has limited access and which groups have access to it?

Risk analysis - Postulate threat agents who wish to harm the assets of the enterprise. Postulate actions they could take. Estimate likelihood.

Security control selection - For the risks laid out in the risk analysis section, describe security controls to mitigate those risks. Use CIS Top 20 controls as guidance, or another framework if you prefer.

Criteria	Description	Points
Asset Identification	Data assets of the enterprise described. Confidentiality, integrity and availability needs described.	20
Risk Analysis	Threat agents for all assets. Possible actions and likelihood for all threat agent/asset pairs. Well thought out and complete listing of threat/action/likelihood/consequence.	20
User Groups and Access Control	Types of users described, e.g. who are trusted users, what data can they access.	10
Controls	Identify controls for each risk. A framework for the suite of controls, e.g. CIS Top 20, is identified.	20

Writing and Quality	Produce a quality product with correct grammar, free of typos, and formatted. Put effort and creativity into the product.	20
Enterprise	Introduce the enterprise. What is their product or industry. What most important to this enterprise?	5
References	Include references, e.g where you got information on what the threat actors and actions are.	5

Grading Policy

Percent	Grade	Grade Points
93.4 - 100	A	4.00
90.0 - 93.3	A-	3.67
86.7 - 89.9	B+	3.33
83.4 - 86.6	B	3.00
80.0 - 83.3	B-	2.67
76.7 - 79.9	C+	2.33
73.4 - 76.6	C	2.00
70.0 - 73.3	C-	1.67
66.7 - 69.9	D+	1.33
63.4 - 66.6	D	1.00
60.0 - 63.3	D-	0.67
0 - 59.9	E	0.00

More information on UF grading policy may be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Students Requiring Accommodations

Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, as early as possible in the semester.

Course Evaluation

Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy

UF students are bound by The Honor Pledge which states, “We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code.

On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment

The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:

- Your academic advisor or Graduate Program Coordinator
- Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.ufl.edu
- Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use

All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy

There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:

Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall*,* 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://care.dso.ufl.edu.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.