

Enterprise Security

Tu 3-4:55, Th 4:05-4:55 , LIT 0121

Academic Term: Spring 2020

Instructor:

Cheryl Resch

Cheryl.resch@ufl.edu

CSE E508

(352) 294 6664 office

3 Credit Hours

Course Pre-Requisites

COP3530

Course Objectives

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

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

Textbook

Enterprise Cybersecurity, How to Build a Successful Cyberdefense Program Against Advanced Threats, Donaldson, Siegel, Williams, Aslam

978-1-4302-6082-0

Attendance Policy, Class Expectations, and Make-Up Policy

Labs:

During the Tuesday meeting time we will be doing activities from <https://nice-challenge.com/>. **Attendance is required. There will be one drop.** Cooperation and mutual support during the labs is allowed and encouraged.

Discussions:

Discussions are conducted through the Canvas Discussion link. Your post will be graded on the effort shown. It doesn't need to be a research paper, but it also should take more than 5 minutes and one google search.

Homeworks:

Homeworks consist of problem solving and will be turned in on Canvas. Per University Honesty Policy, please do your own work.

Paper:

Evaluation of Grades

Assignment	Percentage of Final Grade
Labs (14, 1 drop)	50%
Homeworks 4	15%
Discussions 5	15%
Paper	20%
	100%

Grading Policy

Percent	Grade	Grade Points
93 - 100	A	4.00
90.0 – 92.9	A-	3.67
87 - 89.9	B+	3.33
83 - 86.9	B	3.00
80.0 – 82.9	B-	2.67
77 - 79.9	C+	2.33
73 - 76.9	C	2.00
70.0 – 72.9	C-	1.67
67 - 69.9	D+	1.33
63 - 66.9	D	1.00
60.0 – 62.9	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>

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@ufl.edu

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

Students Requiring Accommodations

Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, <https://www.dso.ufl.edu/drc>) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation

Students are expected to provide feedback on the quality of instruction in this course by completing online evaluations at <https://evaluations.ufl.edu/evals>. Evaluations are typically open during the last two or three weeks of the semester, but students will be given specific times when they are open. Summary results of these assessments are available to students at <https://evaluations.ufl.edu/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://www.dso.ufl.edu/sccr/process/student-conduct-honor-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.

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:

<http://registrar.ufl.edu/catalog0910/policies/regulationferpa.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 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 support, 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://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

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

Week	Dates	Topic	Challenge	Reading	Homework
1	1/7 1/9	Defining the cybersecurity challenge, enterprise cyber security attack sequence		Chapter 1, 2 Enterprise Cyber Security	
2	1/14 1/16	Managing an enterprise cybersecurity program,	“Radical Risk Reduction”	Chapter 14 Enterprise Cyber Security	
3	1/21 1/23	Security policy	“Networking anomalies, policy implementation”	Chapter 4, Appendix D	HW1, Due 1/28
4	1/28 1/30	Inventory and control of hardware and software assets	“Assuring accurate asset inventories”		Discussion 1 – hardware/software inventory products
5	2/4 2/6	Continuous vulnerability management	“Vulnerability scan complete, begin system hardening”		Discussion 2 – vulnerability management products
6	2/11 2/13	Controlled use of administrative privileges Controlled access based on need to know Wireless access control	“Secure roots: domain organization and access controls”		
7	2/18 2/20	Secure configurations	“STIG Solutions”		HW2 , due 2/25
8	2/25 2/27	Maintenance, monitoring, and analysis of audit logs			

9	3/10 3/12	Email and web browser protections	“Malicious mail management”		Discussion 3, Email and web browser management products
10	3/17 3/19	Limitation and control of network ports, protocols and services, boundary defense	“Firewall update: tables for two”		HW3, due 3/24
11	3/24 3/26	Data recovery capabilities, data protection	“Data backup and recovery, definitely worth testing”		Discussion 4, Data back and recovery products
12	3/31 4/2	Security awareness and training program	“Dangerous Drives (Complexity 1)”		Discussion 5, Security awareness and training
13	4/7 4/9	Account monitoring and control	“Networking Anomalies: Policy Implementation”		
14	4/14 4/16	Incident handling	“Malware aftermath clean up”		HW4, due 4/21
15	4/21 4/23	Penetration tests and red team exercise	“Penetration Testing: Bringing passwords up to snuff”		

Grades

Labs – 14 (one drop) 50%

Homeworks – 4 15%

Discussions – 5 15%

Paper 20%