CS-167

CYBERSECURITY DEFENSE

INSTRUCTOR: JIM EDDY

SYLLABUS

Course Information:

- **CRN**: *14691*
- **Term**: *Spring 2018*
- **Format**: *Online, Asynchronous*
- **Learning Management System**: *Blackboard (bb.uvm.edu)*

Contact:

- Jim Eddy
- james.eddy@uvm.edu
- Office Hours: T,W,R 3-4pm 325 Votey
- (802) 656 - 8084

Description:

This course builds on the material covered in *CS166 - Cybersecurity Principles*, with an emphasis on cyber defense. Topics include cyber defense policy, privacy and ethics; network threat defense, intrusion detection and prevention systems, intro to penetration testing, operating system security principles, system/network admin basics, as well as cloud, mobile and IoT security. The course concludes with an overview of security planning, management and incident response. **Prerequisites**: *CS166 - Cybersecurity Principles [CS021 - Computer Programming I: Python, CS 008 - Intro to Website Development]*

Special Note: In order to develop a working knowledge of cybersecurity best practices, it is important to gain an understanding of the techniques used by attackers. Thus, this course presents material that could be used to exploit systems and/or end-users. The assignments are solely designed to be preformed in isolated test environments provided or referred to by the course instructor, and are not to be used on any University computer, or otherwise, with any form of malicious intent. Upon enrollment, students will be expected to sign a statement certifying their commitment to ethical computing practices.

Learning Objectives:

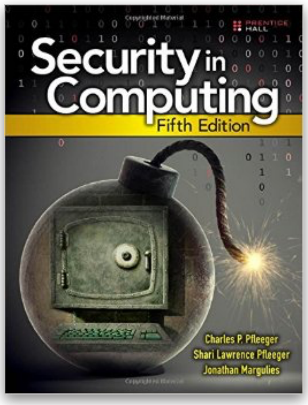
- Understand key concepts related to cyber defense policy, privacy, and ethics
- Gain a solid foundation of network threat defense mechanisms / countermeasures
- Understand the role of intrusion detection and prevention systems
- Understand fundamental security design principles as applied to operating systems
- Gain exposure to common techniques used in penetration testing
- Understand the basic functions performed by system and network administrators
- Understand security concepts in cloud computing models
- Gain exposure to mobile device and Internet of Things (IoT) security
- Be able to develop a comprehensive security strategy, including security planning, business continuity planning, risk analysis and disaster/recovery planning

Class Philosophy:

Everyone is taking this class with the same objective: to learn. This class is designed to have you learn in an online environment with your peers. The expectation is that you are respectful to all, and that you participate and contribute on a regular basis. Stay current with the readings, ask questions often, and help fellow students when they have questions. Please remember: you will get out of this class what you put into it. Let's have a great semester!

Course Materials:

- **Required Textbook**: *Security in Computing, 5/E*, By: Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies.
  ISBN: 9780134085043
- **Reliable Computer** and ability to install virtual machines/Kali Linux, local web server (MAMP), Python 3.x, PHP 5.x, web access, text editor, word processing software, PDF converter, screenshots
- **Web**: Python 3.x Documentation, PHP 5.x Documentation
- **Online Virtual Lab Environment**: Requires $88 access fee
- **Suggested Reading**: *Social Engineering: The Art of Human Hacking,* By Christopher Hadnagy. ISBN: 978-0470639535

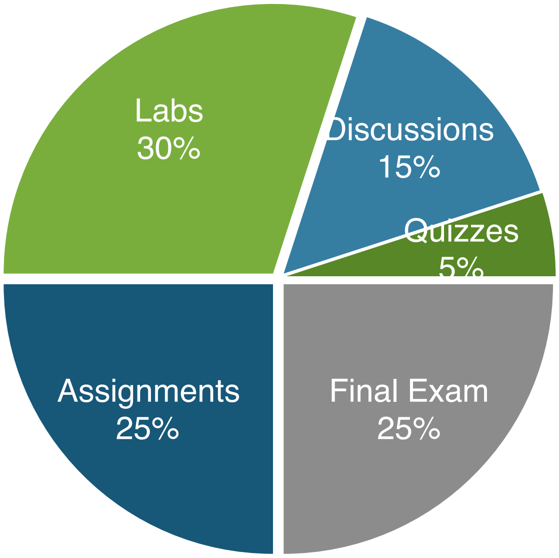


Grading Policy:

The course grade is comprised of a variety of assignments, labs, quizzes, a final exam, and discussions.

For the “discussions” grade, since this is an online course your effort is represented by your activity in the discussion forums. You are required to make a post for each topic within each thread Your post needs to be a minimum of 100 words and be related to the subject in order to let me know that you are staying current with the course material. Your post may be in response to another students’ post, however, it needs to be comprehensive, as simply “I agree” or “good point” - type responses will not satisfy the requirement. Respectful and appropriate posts are the expectation, as is citing your sources.

Any grade appeal must be made within one week of the grade being posted.



Numerical / Letter Grade Conversion

A+	99-100	B+	87-89	C+	77-79	D+	67-69	F	0-59
A	94-98	B	83-86	C	73-76	D	63-66		
A-	90-93	B-	80-82	C-	70-72	D-	60-62		

Modules:

- The following represents the tentative course modules and is subject to change at the discretion of the instructor. Please refer to the assignment due dates posted in Blackboard for the most current schedule.

#	MODULE	ASSIGNMENT	DUE DATE
0	Getting Started	*Introduction to course, syllabus, introduce yourself*	1/23/18
1	Fundamentals of Cyber Defense Policy, Privacy, Legal, and Ethics	*Reading: Chapter 9 - Privacy, Chapter 11 - Legal Issues and Ethics (policies including HIPAA/FERPA, Sarbanes-Oxley, COPPA, US Patriot Act, privacy concepts, ethical issues in computer security)*	1/30/18
2	Introduction to Network Threat Defense	*Reading: Chapter 6 - Networks (strategic defenses, cryptography in network security, IPsec, firewalls, VPNs, DMZs, attack surface and vectors, network monitoring and mapping, network traffic analysis)*	2/06/18
3	Overview of Intrusion Detection and Prevention Systems	*Reading: Chapter 6.8 - Networks/Intrusion Detection and Prevention Systems (IDS, IDS controlled networks, pattern matching and heuristic systems)*	2/13/18

#	MODULE	ASSIGNMENT	DUE DATE
4	Introduction to Penetration Testing	*Reading: Metasploit documentation*	2/20/18
5	Introduction to Operating System Security	*Reading: Chapter 5: Operating Systems (Fundamental Security Design Principles as applied to an OS, including domain separation, process isolation, resource encapsulation, least privilege, processes, threads, virtualization/ hypervisors, file systems, rootkit, patching OS/application security updates)*	2/27/18
6	System and Network Administration Essentials	*Reading: Chapter 6.8 - Network Management (OS installation, user accounts/management, password policies, backup/restoring data, security policy development, network configuration and port security)*	3/06/18
7	Security Concepts in Cloud Computing	*Reading: Chapter 8 - Cloud Computing (cloud services and models, cloud security concepts, cloud security tools and techniques, identify management,)*	3/20/18
8	Mobile Device and IoT Security Basics	*Reading: Chapter 13.1 - The Internet of Things (smart devices, medical devices, program security failures, mobile phones and mobile malware, security in IoT)*	3/27/18
9	Security Planning: Management and Incidents, Risk Analysis	*Reading: Chapter 10 - Management and Incidents (security planning, security life-cycle, business continuity planning, incidents, disaster planning/recovery, risk analysis)*	4/10/18
10	Emerging Topics in Cybersecurity	*Reading: Chapter 13 - Emerging Topics (economics, electronic voting, cyber warfare)*	4/20/18
11	Final Exam	*Cumulative Final Exam, administered through Proctor U (requires exam fee)*	4/27/18

Course Policies:

- **Attendance**: This course is asynchronous, meaning that we will not meet at a particular time each week. Even though we will not meet face-to-face in a physical classroom, participation on all discussion boards is required and paramount to your success.

- **Late Policy**: Late assignments are not accepted without explicit permission from the instructor, and permission can only be granted in the case of an emergency AND provided the request was made prior to the assignment due date. Late work may be subject to a penalty in points at the discretion of the instructor.

- **SAS:** In keeping with University policy, any student with a documented disability interested in utilizing accommodations should contact SAS, the office of Disability Services on campus. SAS works with students and faculty in an interactive process to explore reasonable and appropriate accommodations, which are communicated to faculty in an accommodation letter. All students are strongly encouraged to meet with their faculty to discuss the accommodations they plan to use in each course. Please click on this link, Accommodation Guidelines, to better understand the process. A student's accommodation letter lists those accommodations that will not be implemented until the student meets with their faculty to create a plan. Contact SAS: A170 Living/Learning Center; (802) 656-7753; access@uvm.edu; or www.uvm.edu/access

- **Religious Holidays:** Students have the right to practice the religion of their choice. Each semester students should submit in writing to their instructors by the end of the second full week of classes their documented religious holiday schedule for the semester. Faculty must permit students who miss work for the purpose of religious observance to make up this work. See the Interfaith Calendar. Additional University of Vermont policies may be found at: UVM Policies.

- **Academic Honesty Policy**: The Computer Science Department rigorously enforces the Code of Academic Integrity Policy as outlined in the Code of Rights and Responsibilities and University Policies. At the first suspicion of violation of this policy, the case will be immediately forwarded to the Coordinator of Academic Integrity. The typical sanction for a violation is a grade of an "XF" in the course. A second violation typically results in dismissal from the University.

  Your assignments may be electronically compared to everyone else's. If you assist someone in cheating you are guilty as well (this year or next). You must type and format your assignments yourself, starting an assignment or copying and pasting from someone else's assignment is a case of academic dishonesty and will be treated as such. Each work submitted must be your own work, no collaboration is allowed, except as explicitly defined in the assignment instructions.

  Copying an Exam in any shape or form including but not limited to photocopying, picture taking, writing down or verbally dictating questions and or answers is considered academic dishonesty and will be treated as such. The only external programming code you are allowed to use are the examples provided by the instructor. Any other external code (i.e. found from a Google search, etc.) is considered academic dishonesty and will be treated as such. If you feel the need to use free code or shareware code, please consult with your instructor PRIOR to using it.