Course Syllabus

CNT 5410L: Cyber Operation Lab (Spring 2021)

Instructor: Dr. Cliff Zou (HEC 243), 407-823-5015, czou@cs.ucf.edu

Course Time (for in-campus session): Monday 10:30am-1:20pm

Course Classroom (for in-campus session): Partnership III, Rm 233

Office Hour: TuTh 10:30am-12:00pm, HEC243

Prerequisites: Graduate standing

Required Textbook:

The Basics of Hacking and Penetration Testing (2nd edition) by Patrick Engebretson. Syngress (August 15, 2013). ISBN-10: 0124116442, ISBN-13: 978-0124116443.

Course catalog description and credit hours:

This 3 credit course is titled “CNT 5410L ECS- 3(1,3) Cyber Operations Lab” :PR: IDC 5602 or C.I. Programming, software, and hardware components for cybersecurity operations related to system administration, firewalls, cyber attack, cyber defense, security, secure architectures at network and computer level.

Video Streaming:

We will use UCF Panopto system for video streaming. Recorded videos can be accessed via the “Panopto Video” link in Webcourse. Both face-to-face session (0R01) and online session (0V61) students can access the lecture video in WebCourse. Each class video will be available in the evening after each face-to-face lecture on Monday. Webcourse will be used for assignment release and submission.

Course Learning Objectives:

Cybercrimes and threats of cyber terrorism have rapidly escalated resulting in a tremendous unmet demand for professionals with cyber security training and experience. This course presents a comprehensive overview of cyber security topics. It focuses on various penetration testing methods and corresponding defensive cyber strategies with practice in a virtual machine networking environment that can be run on each student’s own computer. Through extensive hands-on teaching and experimentation, students will be able to learn the most important knowledge and practical skills on networking security, email security, and penetration testing.

Planned Outline of Topics:

1. Course outline and introduction of cybersecurity operation
    1. Course format and outline

    2. Concepts of cyber operation
    3. Ethical hacking and penetration testing
2. Network traffic monitoring and Wireshark tool
    1. Network layer and data link layer traffic monitoring
    2. Wireshark introduction and usage
3. Email spam, phishing and defense
4. Introduction to incident response software - Splunk
5. Introduction and basic operation of Virtual machine (Virtual Box)
6. Kali Linux
    1. Installing Kali Linux virtual machine for later penetration testing
    2. Basic usage of Linux operating system
7. Footprinting
    1. Information gathering process
    2. Gathering detailed target/victim information through various Internet service
8. Port scanning
9. Password cracking (online, offline)
10. Vulnerable machine attack and exploit using Metasploit
11. Internet malware and basic malware analysis
12. Social network security and privacy
13. Common cyberattack defensive techniques

Grading Policy:

The final grade will use +/- policy, i.e., you may get A, A-, B+, B, B- … grade. The final grade will be curved and each student GPA grade is determined not only by the absolute cumulative scores, but also by his/her relative ranking among all students in this class. The tentative grading weights are shown below (subject to change).

Assessment	Percent of Final Grade
Laboratory Assignments (6 times)	16.7% each

Attention to students who receive federal student aid:

All faculty members are required to document students' academic activity at the beginning of each course. In order to document that you began this course, please complete the first created assignment on WebCourse by the end of the first week of classes or as soon as possible after adding the course. Failure to do so may result in a delay in the disbursement of your financial aid. This first homework assignment will not be graded or counted in final grading.