CIS6395: Incidents Response Technologies (Fall 2021)

Instructor: Dr. Cliff Zou (HEC 243), changchun.zou@ucf.edu, office phone: 407-823-5015

Course Time: Monday/Wednesday 10:30am-11:45am, Eng1-384 (real-time lecture and recording)

[Note]: No matter which session you have registered, you have freedom to either come to classroom (Eng1-384), or join, or not join the real-time Zoom lecturing remotely. Lecturing videos (Zoom recording and Panopto recording) are available for everyone within one hour after each lecturing time.

Course Classroom: Eng1-384 classroom is used for in-campus lecturing; at the same time, we rely on Zoom-based real-time lecture recording two times per week on course scheduled time.

Office Hour: Monday/Wednesday 12pm-1:30pm, Office is HEC-243, You can come to my office, call office phone (407-823-5015) or join office hour Zoom meeting via webcourse's Zoom link:
https://ucf.zoom.us/j/95903321935?pwd=eFBHVnFuVjVRaHZFWmhMTVRIUnBpQT09

Prerequisites: CDA 5106 or COT 5405, or MSDF major

Knowledge on computer architecture, data structure, and networking;
Knowledge of basic usage of Linux machine.

Required Textbook: Not required

Reference books (not required):

1. The Basics of Hacking and Penetration Testing (2nd edition) by Patrick Engebretson (2013). ISBN-10: 0124116442, ISBN-13: 978-0124116443
2. Network Forensics: Tracking Hackers through Cyberspace, by Sherri Davidoff and Jonathan Ham (2012). ISBN-10: 0132564718, ISBN-13: 978-0132564717

Zoom-based real-time lecturing and video streaming:

We will use WebCourse's integrated Zoom system for real-time online lecturing and video streaming. Both face-to-face session (0V01) and online session (0V61) students have the freedom to either join or not join in the real-time Zoom lecturing on the lecture time via the "Zoom" tab link in the webcourse (Monday/Wednesday 10:30am-11:45am). Everyone can access the recorded lecture video via the "Zoom" tab link in Webcourse after each lecture time (clicking the 'Cloud Recordings' tab). Webcourse will also be used for lecture content dissemination, assignment release and submission.

Course catalog description and credit hours:

3(3,0). PR: Digital Forensics MS major or CDA 5106 or COT 5405. This course covers security incidents and intrusions. Topics include: identifying and categorizing incidents, responding to incidents, log analysis, network traffic analysis, and tools.

Student Learning Outcomes:

(a) Understand basic knowledge and procedure on handling with cyber security attack, data breach, data damage incidents;

(b) Able to conduct basic forensic analysis of Windows and Linux systems;

(c) Able to use popular tools in analyzing compromised systems and conducting static and dynamic malware analysis;

(d) Able to conduct basic penetration testing (information gathering and exploitation);

(e) Able to use Wireshark for network traffic capture and analysis, and use Splunk software to process and analyze incident response security logs.

Planned Outline of Topics:

- Course outline and introduction
- Background knowledge: Basic Networking Principles
- Get familiar with VirtualBox Virtual Machine software and installation of Kali Linux VM
- Linux basic usage and administration
- Network traffic monitoring and Wireshark usage
- Malware Incident Response
    - Static Analysis
    - Dynamic Analysis
- Basic Reverse Engineering
- Incident Response and Event Log Analysis
- Use Splunk for Incident Response and Event Log Analysis
- Penetration Testing
    - Information gathering
    - Scanning
    - Exploitation
- System hardening: example of securing a vulnerable virtual machine system

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
Regular Assignments (4)	60%
Mid-term Exam (1)	20%
Final Exam (1)	20%

Assignment Submission and Exam Format:

All regular assignments and mid-term/final exams are released on webCourse Assignment section. Regular assignments will be due one week to 10 days after releasing time. Midterm exam and final exam can be treated as special homework assignments where they are due 24 hours after releasing time; there is no need to come to campus or use proctor for completing exams.

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.