# CIS6395: Incidents Response Technologies (Spring 2016)

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

**Course Time:** Monday 12pm-1:15pm (for face-to-face session)

**Course Classroom**: Eng1-386A

**Course Webpage:** http://www.cs.ucf.edu/~czou/CIS6395-16/

**Office Hour**: MoWe 9:30am-11:30am, HEC243

**Prerequisites:** CGS 5131 and CNT 6418, or C.I.
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. Hacker Techniques, Tools, And Incident Handling (2nd Edition) by Sean-Philip Oriyano. Jones & Bartlett Learning (2013). ISBN-13: 9781284031713, ISBN-10:1284031713

**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. Each class video will be available in late afternoon after each face-to-face lecture on Monday and Wednesday. Webcourse will be used for assignment release and submission.

**Course catalog description and credit hours:**

3(3,0). PR: CGS 5131 and CNT 6418, or C.I. This course covers security incidents and intrusions. Topics include: identifying and categorizing incidents, responding to incidents, log analysis, network traffic analysis, and tools.

**Course Learning Objectives:**

(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 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
- Windows Incident Response and Event Log Analysis
- Linux Incident Response and Event Log Analysis
- Penetration Testing
    - Information gathering
    - Scanning
    - Exploitation

**Grading Policy:**

The final grade will use +/- policy, i.e., you may get A, A-, B+, B, B- … grade. The tentative grading weights are shown below (subject to change).

| Assessment | Percent of Final Grade |
|---|---|
| Regular Assignments (5) | 65% |
| Mid-term Exam (1) | 15% |
| Final Exam (1) | 20% |

**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.