# CIST 1327 TOPICS in CIS&T:
# Intrusion Detection & Incident Response
**Fall 2016**

**Lecture hours and locations:** M W 11:30 AM - 12:45 PM HANGR00124
**Instructor:** Shushan Zhao
**Office:** Swarts Hall 160
**Office Phone:** 814-362-7639
**E-mail:** shushanz@pitt.edu;
**Office Hours:** 3:30 PM – 5:00 PM Tuesday/Thursday, and by appointment.
**Prerequisites:** Upper level standing

**Course Description:**
In this course students will learn what it takes to be prepared for intrusion, what it takes to detect the instruction, and eradicate it, including: Introduction of intrusion detection & protection, and incident response concepts, familiarity with common Intrusion prevention system (IPS), Intrusion detection system (IDS) and Intrusion responses (IR) approaches and their applications, understanding of practical aspects of implementing and managing intrusion protection, detection systems, and familiarity with the operations of effective incident response processes and organizations.

Key topics include:
- Understanding How Internet and TCP/IP Networks Works
- Types of Attacks
- Installation and configuration of firewalls, IDS
- Prevention against Attacks
- Security policies

**Course Objectives:**

After taking this course, students will understand various sources of intrusion and attacks to computer systems, and most importantly the principles of TCP/IP networks and network intrusions. They will also learn how to prevent and respond to intrusions, and be able to configure properly operating systems, install Intrusion prevention systems and Intrusion detection systems on Windows/Linux against intrusions.

**Textbooks**:
Network Defense and Countermeasures: Principles and Practices, 2nd Edition
Author: William Easttom
Publisher: Pearson
ISBN-13: 978-0789750945
ISBN-10: 0789750945

**Grading and Evaluation Criteria**

Grading will be based on:

| | |
|---|---|
| In-class quizzes | 10% |
| Homework Assignments | 30% |
| Examination | 60% |

| % of points earned | Grade |
|---|---|
| 97-100 | A+ |
| 93-96 | A |
| 90-92 | A- |
| 87-89 | B+ |
| 84-86 | B |
| 80-83 | B- |
| 77-79 | C+ |
| 74-76 | C |
| 70-73 | C- |
| 67-69 | D+ |
| 64-67 | D |
| Below 64 | F |

## Tentative Course Outline

| Week | Topics | Notes |
|---|---|---|
| **1** | Introduction to network security, intrusion detection & incident response. | |
| **2** | Types of threads and attacks | |
| **3** | Fundamentals of firewalls | |
| **4** | Fundamentals of IDS | |
| **5** | Intrusion responses (IR) | |
| **6** | Detecting & Defending against Malware | |
| **7** | Firewall practical applications --- Windows & Linux firewalls | |
| **8** | IDS practical applications --- snort | |
| **9** | IPS and Operating system hardening --- Windows | |
| **10** | IPS and Operating system hardening --- Linux | |
| **11** | Network traffic capture and analysis --- tcpdump & wireshark | |
| **12** | Encryption fundamentals | |
| **13** | Secure communication protocols & Network Security -I | |
| **14** | Secure communication protocols & Network Security -II | |
| **15** | Time for Student Presentations | |

There will be 4 assignments and a presentation.
Presentation topic is "A Case Study of Intrusion Detection & Incident Response"

## Ethics Note

The tools and techniques you learn in this class should be used with care and prudence. What you learn in this class is to be used in an ethical manner. The tools and techniques should NEVER be used to break the law. You are responsible for your own behavior!

## CourseWeb

Supplementary information for the course is available on the class courseweb site. The Web site contains class notes, PowerPoint slides, class announcements, the course syllabus, and other information for the course.

## E-Mail

All students should be checking their Pitt e-mail account on a regular basis. If you have any questions about the course or need assistance, please contact me in person or by telephone during office hours; or by e-mail at any time.

## Attendance

Absence from this class is a serious matter and should be discussed with me in advance. Excessive absences will be reason enough to drop your grade one FULL letter.
Arriving late to class repeatedly is a sign of disrespect, both to me and to your classmates. It is expected that students show respect for the class by turning off cell phones, by not packing up personal belongings until after I have indicated that the class is over, and by acting with civility.

## Student Opinion of Teaching Surveys

Students in this class will be asked to complete a *Student Opinion of Teaching Survey*. Surveys will be sent via Pitt email and appear on your CourseWeb landing page during the last three weeks of class meeting days. Your responses are anonymous. Please take time to thoughtfully respond, your feedback is important to me. Read more about *Student Opinion of Teaching Surveys*.

## University Policies:

*Academic Integrity*

Students in this course will be expected to comply with the University of Pittsburgh's Policy on Academic Integrity. Any student suspected of violating this obligation for any reason during the semester will be required to participate in the procedural process, initiated at the instructor level, as outlined in the University Guidelines on Academic Integrity. This may include, but is not limited to, the confiscation of the examination of any individual suspected of violating University Policy. Furthermore, no student may bring any unauthorized materials to an exam, including dictionaries and programmable calculators.

*Disability Services*

If you have a disability for which you are or may be requesting an accommodation, you are encouraged to contact both your instructor and the Academic Success Center's Disability Resources and Services Office (218 Hanley Library, 814-362-7609) as early as possible in the term. DRS will verify your disability and determine reasonable accommodations for this course.

*Copyright Notice*

Course materials may be protected by copyright. United States copyright law, 17 USC section 101, et seq., in addition to University policy and procedures, prohibit unauthorized duplication or retransmission of course materials. See Library of Congress Copyright Office and the University Copyright Policy.

## Statement on Classroom Recording

To ensure the free and open discussion of ideas, students may not record classroom lectures, discussion and/or activities without the advance written permission of the instructor, and any such recording properly approved in advance can be used solely for the student's own private use.