Intrusion Detection

CSC 433B (Online)
Fall 2013

Professor: Lucas Vespa
Office: UHB 3119
Email: lvesp2@uis.edu

Course Overview

Intrusion Detections Systems (IDS) are an integral element in Information System Security designs. IDS require continuing development in both the manual and automated network traffic analysis techniques used to create signatures for identifying malicious traffic. This course discusses an overview of current network protocols and how misuse of these protocols can be systematically identified. This course also discusses tools to aid in the capture and analysis of network traffic (*Windump*/*Wireshark*), tools used to test an IDS (*NMAP*), as well as a popular open-source IDS (*Snort*) and tools to generate raw packets (*Scapy*).

Required Textbooks

Network Intrusion Detection (3rd Edition) by Stephen Northcutt and Judy Novak
ISBN 0735712654

Recommended supplemental resources cited in the *"Course Information"* and *"Course Software"* sections of the Blackboard course.

Grading

This course consists of 16 modules (approximately one module per week). For each module you will review course materials such as reading from the required textbook and watching PowerPoint and video lectures. After reviewing the relevant material, most modules have a quiz and associated assignment. In the last several weeks of the course, you will also complete a final project which consists of configuring, programming and implementing a software based Network Intrusion Detection System. The table below details the grading weight of the quizzes, assignments and final project.

Reasonable accommodations are available for students who have a documented disability. Please notify the instructor during the first week of class of any accommodations needed for the course. Late notification may cause the requested accommodations to be unavailable. All accommodations must be approved through the Office of Disability Services (ODS) in the Human Resources Building (HRB), Room 80, 217-206-6666.

Quizzes	25%
Assignments	50%
Final Project	25%

Course Delivery Method

Blackboard will be the delivery method for this course. In order to keep up with what tasks you need to complete, you must consistently check the **Announcements** Section of our Blackboard course. I will post an announcement every time there is a new assignment, quiz, or any important piece of information you need to do well in this course.

Expected Course Topics/Schedule and Associated Course Material Sources

Week	Topic	Source Information
1	Intrusion Detection Overview	Introductory Whiteboard Video Lecture and PowerPoint Lectures
2	IP Concepts (v4 and v6)	Chapter 1Readings and PowerPoint Lectures
3	Introduction to TCP Dump and TCP	Chapter 2 Readings and PowerPoint Lectures
4	Fragmentation	Chapter 3 Readings and PowerPoint Lectures
5	ICMP	Chapter 4 Readings and PowerPoint Lectures
6	Stimulus and Response	Chapter 5 Readings and PowerPoint Lectures
7	DNS	Chapter 6 Readings and PowerPoint Lectures
8-10	Real World Traffic Analysis	Chapter 7-11 Readings and PowerPoint Lectures
11	Nmap Tool	PowerPoint Lectures / Software Documentation
12	Introduction to Snort and Snort Rules	Chapter 13-14 Readings and PowerPoint Lectures
13	Deep Packet Inspection Methods	Selected Papers and Whiteboard Video Lectures
14	Fall Break	-----
15	Mitnick Attack / Generating Raw Packets	Chapter 15 Readings and PowerPoint and Video Lectures
16	Architectural Issues and Packet Generate	Chapter 16 Readings and PowerPoint Lectures

Ethical Behavior

In this course we may potentially use software tools which have potential for malicious use. It is expected that all students in this course will conduct their behavior in an ethical manner. Please observe and follow the following rules written by the Computer Ethics Institute: http://cpsr.org/issues/ethics/cei/

Plagiarism

Plagiarism is not acceptable under any circumstance. All students in this course will be held to the highest integrity standards. If you are caught plagiarizing (copying material without quoting and citing the material source) you will receive a failing grade for the course. Plagiarism recognition software is used by the instructor of this course to aid in the discovery of copied material. If you have questions about what will and will not be considered plagiarism please email me before submitting the material in question (lvesp2@uis.edu).

Notes

- Please contact me immediately with any questions or concerns as soon as they arise. I am available almost anytime to help with your concerns. You may contact me through email. I also am more than willing to (and often do) set up online video conferences with students. My preferred software for this is Vsee (http://vsee.com/) but I am willing to consider other options as well.
- Backup all of your work constantly. (Hint: Email files to yourself at every stage of work), use an external storage method and cloud storage.