CPSC 4166 Intrusion Detection and Prevention
Spring 2018

Instructor information:
Name: Jianhua Yang, *Ph.D.*
Office: Center for Commerce and Technology (CCT) Room 440
Office hours: TBA;
Meeting hours and classroom: TR 9:30am – 10:45am at CCT123
Email: yang_jianhua@columbusstate.edu
Website: http://csc.ColumbusState.edu/yang
Office Phone: 706/507-8180; School Phone: 706-568 2410; School Fax: 706-565 3529

Course Description:
The capstone course delivers the tenets of intrusion detection and prevention, specifically focus on stepping-stone intrusion detection and prevention. Intrusion Detection focuses on the methods to detect attempts (attacks or intrusions) to compromise the confidentiality, integrity or availability of an information system. And intrusion prevention focuses on the techniques to block such intrusions. It includes host-based intrusion detection, network-based intrusion detection, network traffic sniffing tools, stepping-stone intrusion detection, packet round-trip time, detection performance management, hackers' evasion techniques, and attacks via TOR.

Textbook:
No required textbook, but some research papers.

Learning objectives:

1. To understand the basic intrusion and prevention techniques
2. To identify intrusion detection systems and their signatures
3. To understand different stepping-stone intrusion approaches
4. To make an intelligent choice to defend a computer/network system
5. To become intrusion detection/prevention or security analysts
6. To be able to develop a tool to detect/prevent stepping-stone intrusion
7. To be familiar with at least one intrusion detection tool, such as Snort

Learning outcome:

1. Students will, upon completion of this course, have a broad understanding and knowledge skills in network security and stepping-stone intrusion.
    a. Students will have a conceptual understanding and practical experience in intrusion;
    b. Students will have a strong foundation about network traffic representation;
    c. Students will have a strong understanding of TCP/IP protocols;
    d. Students will have a conceptual and fundamental understanding of computer network, information assurance, and system security;
    e. Students will have a certain understanding in design, analysis and complexity evaluation of stepping-stone intrusion detection system;
    f. Students will have practical experience in matching TCP/IP packets and protecting computer system and preventing stepping-stone attacks.
2. Students will have courses that focus on in depth understanding of selected areas of network security, intrusion detection and prevention.
3. Students will be able to communicate effectively both orally and in written reports.

4. Students will have the knowledge and skills to pursue careers in industry and/or higher education degree programs.
5. Students will be able to integrate their knowledge and skills into evolving technologies in computer network security, and stepping-stone intrusion detection and prevention.

Major Topics:

1. Fundamentals in intrusion detection and prevention
2. Host-based intrusion detection
3. Network-based intrusion detection
4. Network traffic sniffing
5. Network traffic manipulation
6. Stepping-stone intrusion
7. Stepping-stone intrusion detection
8. Stepping-stone intrusion prevention
9. Packet round-trip time
10. Detection performance measurement

Course Methods

1. Student will study the topics independently under instructor's supervision.
2. Laboratory experiences will be part of the course.
3. Students will be expected to complete hands-on exercises and a series of programming assignments.

Student Responsibilities

1. Study each topic via PPT provided.
2. Complete all reading assignments and all homework assignments.
3. Ask the instructor questions.
4. Send the instructor e–mail with both comments and questions.
5. Make class presentation

Instructor Responsibilities

1. Supervise student to learn the course material.
2. Assign appropriate homework that illustrates the concepts of the course, and grade and return the homework in a timely manner with adequate explanation.
3. Give tests over the material and grade and return the tests in a timely manner
4. Provide a website that supports the course.
5. Provide at least four hours of office time primarily designated for assistance of students in this class, at times expected to be convenient for the students. It is expected that the instructor be available to the students during these hours.
6. Reply promptly (within one business day) to all student e–mail communications.

COURSE EVALUATION

GRADED LEARNING ACTIVITIES	**Percentage**	**Points**
Chapter Test		40
Hands-on labs		30
Project		30

TOTAL		**100**

Percentage Range	**Final Grade**
90-100%	A
80-89%	B
70-79%	C
60-69%	D
59% and below	F

CSU Academic Honesty Policy
Academic dishonesty includes, but is not limited to, activities such as cheating and plagiarism (**http://aa.colstate.edu/advising/a.asp#AcademicDishonestyAcademicMisconduct**). It is a basis for disciplinary action. Any work turned in for individual credit must be entirely the work of the student submitting the work. All work must be your own. [For group projects, the work must be done only by members of the group.] You may share ideas but submitting identical assignments (for example) will be considered cheating. You may discuss the material in the course and help one another with debugging; however, any work you hand in for a grade must be your own. A simple way to avoid inadvertent plagiarism is to talk about the assignments, but don't read each other's work or write solutions together unless otherwise directed by your instructor. For your own protection, keep scratch paper and old versions of assignments to establish ownership, until after the assignment has been graded and returned to you. If you have any questions about this, please see your instructor immediately. For assignments, access to notes, the course textbooks, books and other publications is allowed. All work that is not your own, MUST be properly cited. This includes any material found on the Internet. Stealing or giving or receiving any code, diagrams, drawings, text or designs from another person (CSU or non-CSU, including the Internet) is not allowed. Having access to another person's work on the computer system or giving access to your work to another person is not allowed. It is your responsibility to prevent others from having unauthorized access to your work.

No cheating in any form will be tolerated. Penalties for academic dishonesty may include a zero grade on the assignment or exam/quiz, a failing grade for the course, suspension from the Computer Science program, and dismissal from the program. All instances of cheating will be documented in writing with a copy placed in the Department’s files. Students will be expected to discuss the academic misconduct with the faculty member and the chairperson.

If you have any questions about what is plagiarism, check the following sites:

- Plagiarism: What It is and How to Recognize and Avoid It
- Avoiding Plagiarism?
- Avoiding Plagiarism
- Avoiding Plagiarism - MASTERING THE ART OF SCHOLARSHIP

CSU ADA statement
If you have a documented disability as described by the Rehabilitation Act of 1973 (P.L. 933-112 Section 504) and Americans with Disabilities Act (ADA) and would like to request academic and/or physical accommodations please contact Joy Norman at the Office of Disability Services in the Center for Academic Support and Student Retention, Tucker Hall (706) 568-2330, as soon as

possible. Course requirements will not be waived but reasonable accommodations may be provided as appropriate.

Week	Topic	Student Activity	Lab/Project
1 (1/23)	Class Overview		
1 (1/25)	Lecture 1: Introduction (slide 1-23)		
2 (1/30)	Lecture 1: Introduction (slide: 24-43)		
2 (2/1)	Lecture 1: Introduction (slide: 44-59)		
3 (2/6)	Lecture 2: Host Intrusion Detection (slide: 1-23)	Test 1	
3 (2/8)	Lecture 2: Host Intrusion Detection (slide: 24-45)		
4 (2/13)	Lecture 3: Network Intrusion Detection (slide: 1-18)	Test 2	
4 (2/15)	Lecture 3: Network Intrusion Detection (slide: 19-36)		
5 (2/20)	Lecture 3: Network Intrusion Detection (slide: 37-53)		Lab 1
5 (2/22)	Lecture 4: Network Traffic Sniffing (slide: 1-21)	Test 3	
6 (2/27)	Lecture 4: Network Traffic Sniffing (slide: 22-49)		Lab 2
6 (3/1)	Lecture 4: Network Traffic Sniffing (slide: 50-70)		
7 (3/6)	Lecture 5: Stepping-stone Intrusion Detection (slide: 1-20)	Test 4	Lab 3
7 (3/8)	Lecture 5: Stepping-stone Intrusion Detection (slide: 21-40)		
8 (3/13)	Lecture 5: Stepping-stone Intrusion Detection (slide: 41-69)		
8 (3/15)	Lecture 5: Stepping-stone Intrusion Detection (slide: 70-89)	Test 5	Lab 4
9 (3/19-25)	**Spring Break (No Class)**		**Project starts**
10 (3/27)	Lecture 6: Packet Round-Trip time (slide: 1-25)		
10 (3/29)	Lecture 6: Packet Round-Trip time (slide: 26-52)		
11 (4/3)	Lecture 7: Performance Measurement (slide: 1-16)	Test 6	Lab 5
11 (4/5)	Lecture 7: Performance Measurement		

	(slide: 17-32)		
12 (4/10)	Lecture 8: Hacker’s Evasion Techniques (slide: 1-19)	Test 7	Lab 6
12 (4/12)	Lecture 8: Hacker’s Evasion Techniques (slide: 20-39)		
13 (4/17)	Lecture 8: Hacker’s Evasion Techniques (slide: 40-59)		
13 (4/19)	Lecture 9: Attacks via TOR (slide: 1-18)	Test 8	**Project Ends**
14 (4/24)	Final Project Presentation	Test 9	
14 (4/26)	Final Project Presentation		
15 (5/1)	Final Project Presentation		
15 (5/3)	Final Project Presentation		
16 (5/7-12)	Reading Day (5/7) Final Exam Time (5/10)		