CPSC 4166 Intrusion Detection and Prevention
Spring 2019

Instructor information:
Name: Jianhua Yang, *Ph.D.*
Office: Center for Commerce and Technology (CCT) Room 440
Office hours: TBA;
Meeting hours and classroom: TR 6:00pm – 07:15pm 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.

Reference book:
Network Intrusion Detection, 3rd edition, Stephen Northcutt, Judy Novak, New Riders Publishing, 2002, ISBN : 0-73571-265-4.

Other Required Materials:

1. Knowing how to use Scanner and network traffic sniffing tools.
2. Install snort to your computer
3. Install ssh client to your computer

Instructional Materials:

1. The copyright of all the PPT slides from module 1 to Lecture 8 belongs to the instructor Jianhua Yang. We are also permitted by the publisher and the authors to use the materials in this class.

2. All the papers in Handout folder at D2L are downloaded from portal of CSU library. CSU has the permission to use them for academic purpose.

3. All the programming hands-on assignments are designed by the instructor.

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, prevention, and TCP/IP
2. Network traffic sniffing and analysis
3. Analyzing network traffic to detect intrusion
4. Using snort to detect intrusion
5. Stepping-stone intrusion detection
6. Packet matching and round-trip time
7. Intrusion infrastructure

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 quizzes

Student Responsibilities

1. Post your question online and critiques on your peer's question.

2. Form your own group by picking up your groupmate freely to do the collaborative project if we have one.

3. Hands-on assignments and term project if there is any:

    - All assignments must be typed other than hand-written and must be submitted in one package (zip file).

- Assignments and term projects are due exactly at the required time. **Late submission is accepted, but 10 points penalty per day** is applied.
- Submit the softcopy of the assignments through your D2L account.
- Any questions or complaints regarding the grading of an assignment or test must be raised **within one week** after the score or the graded assignment is made available.

4. There are no make-up tests except in verified medical emergencies and with immediate notification.

5. Providing answers for any examination when not specifically authorized by the instructor to do so, or, informing any person or persons of the contents of any examination prior to the time the examination is given is considered cheating.

6. Penalty for cheating will be extremely severe. Use your best judgment. If you are not sure about certain activities, consult the instructor. **Standard academic honesty procedure will be followed for cheating and active cheating automatically results F in the final grade.** Please http://aa.columbusstate.edu/advising/a.htm#Academic Dishonesty/Academic Misconduct for additional information.

7. Pay very careful attention to your email correspondence. It reflects your communication skills. Avoid use non-standard English such as "how r u?" in your email message. In addition, I recommend you put the class number **CPSC 4166** and a brief summary of your question in your email subject. For example,

   ```
   Subject: CPSC 4166 A question on using vulnerability scanner
   ```

   I immediately discard anonymous emails.

Instructor Responsibilities

1. Maintain course materials at D2L including hands-on labs, quizzes, PPT slides for each module, and online discussion.
2. Give class lectures and demonstration on the course material.
3. Assign appropriate homework that illustrates the concepts of the course, and grade and return the homework in a timely manner with adequate explanation.
4. Give tests over the material and grade and return the tests in three days after the due date.
5. Provide a website that supports the course.
6. Reply all student e–mail communications within two business days.
7. Student posting will be handled in 24 hours
8. Student Assignment/hands-labs will be graded in 3 business days; comments and feedback will be given in two business days
9. All the lecture tests/quizzes will be graded in time by the system, but the feedback will be given by the instructor in one business day
10. Collaborative project if there is any will be graded and returned in four business days

Etiquette Expectations

1. Respect each other in terms of opinions and debate issues, not personalities.
2. Do not use online discussion ROOM as a chat room. The discussion room can only allow you to discuss any questions related to this class, other than anything else.
3. Do not make sexist or racial remarks in your any question of discussion.
4. Do not curse as it is offensive to some.
5. Do not make religious remarks unless they are germane to the course material.
6. We reserve the right to make new ground rules as we progress. Feel free to ask any questions that you might have if you are unclear about anything in this online class. You can always

send a note to my email.

7. Assignment questions may be discussed in the online discussion room, but nobody is allowed to post any solutions for any questions included in the assignments of the class.

COURSE EVALUATION

GRADED LEARNING ACTIVITIES	Percentage	Points
Module quiz		20
Hands-on labs		20
Class questions and attendance		10
Midterm Exam		20
Final Exam		30
TOTAL		**100**

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

ADMINISTRATIVE Policies AND ACADEMIC RESOURCES

CSU DISABILITY POLICY (ADA and 504 Statement)

If you have a documented disability as described by the Americans with Disabilities Act (ADA) and the Rehabilitation Act of 1973, Section 504, you may be eligible to receive accommodations to assist in programmatic and/or physical accessibility. We recommend that you contact the Center for Accommodation and Access located in Schuster Student Success Center, **Room 221, 706-507-8755** as soon as possible. The Center for Accommodation and Access can assist you in formulating a reasonable accommodation plan and in providing support. Course requirements will not be waived but accommodations may be able to assist you to meet the requirements. Technical support may also be available to meet your specific need.

ACADEMIC INTEGRITY

All students are expected to recognize and uphold standards of intellectual and academic integrity. As a basic and minimum standard of conduct in academic matters that students be honest and that they submit for credit only the products of their own efforts. Both the ideals of scholarship and the need for fairness require that all dishonest work be rejected as a basis for academic credit. They also

require that students refrain from any and all forms of dishonorable or unethical conduct related to their academic work.
Students are expected to comply with the provisions of Section III, "Student Responsibilities," of the Columbus State University Student Handbook. This specifically includes the sections on "Academic Irregularity," and "Conduct Irregularity." In particular, the Columbus State University Student Handbook states:
"No student shall give or receive assistance in the preparation of any assignment, essay, laboratory report, or examination to be submitted as a requirement for any academic course in such a way that the submitted work can no longer be considered the personal effort of the student submitting the work."
Examples of Academic Dishonesty include but are not limited to: Plagiarism (see definition below), giving or receiving unauthorized assistance on exams, quizzes, class assignments or projects, unauthorized collaboration, multiple submissions (in whole or part) of work that has been previously submitted for credit.
Plagiarism is any attempt to represent the work or ideas of someone else as your own. This includes purchasing or obtaining papers from any person and turning them in as your own. It also includes the use of paraphrases or quotes from a published source without properly citing the source. All written assignments may be submitted for textual similarity review to Turnitin.com for the detection of plagiarism.
Please be aware that anyone caught cheating or plagiarizing in this class will receive a "0" for the assignment/exam and may receive a "0" for the course.
WRITING CENTER
Please get assistance for your academic progress from CSU Writing Center.
TUTORING Service
Tutoring Center in TSYS School of Computer Science can help you on any questions you have in the class online. Please follow the process covered in Chapter 0 to obtain the service to help you to reach academic goal.
CSU LIBRARY
You can always find what you need from CSU Library.
TESTING CENTER
The CSU Testing Center is always ready to serve our students. **The Center** is a nationally certified test center that provides institutional testing, professional certification and licensure tests, other academic tests, and test administration services for current and prospective CSU students, students of other educational institutions, and the community at large. The Testing Center adheres to the Professional Standards and Guidelines for Post-Secondary Test Centers, as adopted by the National College Testing Association (NCTA), to the best of its ability.
COUNSELING CENTER
CSU counselling center can provide counseling services to assist students with various life concerns. Click the links for more information or call the Counseling Center at 706-507-8740 to schedule an appointment.
CAREER DEVELOPMENT CENTER
The Center for Career Development at CSU strives to enhance student success through the development and implementation of experiential learning opportunities aimed at career preparation and life skills competencies.
ADMISSION
CSU Admission Service is here!
FINICIAL AID
The Financial Aid and Enrollment Service Center teams are here to help you through the financial aid process and help you meet your educational costs. Please access it by clicking here.
REGISTRA'S OFFICE
The Office of the Registrar develops and implements registration procedures and maintains student record information that allows us to maximize services to students, faculty, and staff.

STUDENT COMPLAINT PROCESS
Information and resources for student complaints and academic appeals are located at the following link on the Columbus State University website http://aa.columbusstate.edu/appeals/.
COURSE ATTENDANCE POLICY
Students are required to take part in the discussion related to each chapter through D2L.

TECHNICAL RESOURCES

HARDWARE REQUIREMENTS

How do I know if my computer will work with D2L?

SOFTWARE REQUIREMENTS

An- office suite such as Microsoft Office or Open Office

- To open PDF files you might need Acrobat Reader
- Browser Plugins (Pdf files, QuickTime files, Mp4 files) can be usually be obtained at the browsers website.
  Google Chrome
  Firefox
  Safari
  Internet Explorer (Caution: IE is often problematic for D2L-CougarVIEW)
  ASP.NET Visual Studio 2017.

If you need technical support or need assistance configuring your computer, you can refer to the link located in the "Support Resources" widget located on your "My Home" and your "Course Home" pages. If you cannot solve your problem after reviewing the knowledge base help pages, you can call help center 24-7 and talk to a Help Center agent. The number is 1-855-772-0423.

Accessibility Statement

CSU commits to providing accessibility service to all disabilities of accessing the learning management system, and all required technologies, such as D2L, NetLab.

COLLEGE SPECIFIC SECTION

N/A

Tentative Schedule

Refer to Course Schedule File.