IT-2730: INTRUSION DETECTION/PREVENTION SYSTEMS FUNDAMENTALS

Cuyahoga Community College

Viewing: IT-2730 : Intrusion Detection/Prevention Systems Fundamentals

Board of Trustees:
January 2018

Academic Term:
Fall 2018

Subject Code
IT - Information Technology

Course Number:
2730

Title:
Intrusion Detection/Prevention Systems Fundamentals

Catalog Description:
Covers the design, implementation, and administration of Intrusion Detection/Prevention Systems. Includes practical, hands-on experience working with these systems and analysis various attack signatures and the network traffic these systems collect.

Credit Hour(s):
3

Lecture Hour(s):
2

Lab Hour(s):
2

Requisites

Prerequisite and Corequisite

I. ACADEMIC CREDIT

Academic Credit According to the Ohio Department of Higher Education, one (1) semester hour of college credit will be awarded for each lecture hour. Students will be expected to work on out-of-class assignments on a regular basis which, over the length of the course, would normally average two hours of out-of-class study for each hour of formal class activity. For laboratory hours, one (1) credit shall be awarded for a minimum of three laboratory hours in a standard week for which little or no out-of-class study is required since three hours will be in the lab (i.e. Laboratory 03 hours). Whereas, one (1) credit shall be awarded for a minimum of two laboratory hours in a standard week, if supplemented by out-of-class assignments which would normally average one hour of out-of-class study preparing for or following up the laboratory experience (i.e. Laboratory 02 hours). Credit is also awarded for other hours such as directed practice, practicum, cooperative work experience, and field experience. The number of hours required to receive credit is listed under Other Hours on the syllabus. The number of credit hours for lecture, lab and other hours are listed at the beginning of the syllabus. Make sure you can prioritize your time accordingly. Proper planning, prioritization and dedication will enhance your success in this course. The standard expectation for an online course is that you will spend 3 hours per week for each credit hour.

II. ACCESSIBILITY STATEMENT

If you need any special course adaptations or accommodations because of a documented disability, please notify your instructor within a reasonable length of time, preferably the first week of the term with formal notice of that need (i.e. an official letter from the Student Accessibility Services (SAS) office). Accommodations will not be made retroactively. For specific information pertaining to ADA accommodation, please contact your campus SAS office or visit online at https://www.tri-c.edu/student-accessibility-services/. Blackboard accessibility information is available at http://access.blackboard.com.
III. ATTENDANCE TRACKING

Regular class attendance is expected. Tri-C is required by law to verify the enrollment of students who participate in federal Title IV student aid programs and/or who receive educational benefits through other funding sources. Eligibility for federal student financial aid is based in part on enrollment status.

Students who do not attend classes for the entire term are required to withdraw from the course(s). Additionally, students who withdraw from a course or stop attending class without officially withdrawing may be required to return all or a portion of their financial aid based on the date of last attendance. Students who do not attend the full session are responsible for withdrawing from the course(s).

Tri-C is responsible for identifying students who have not attended a course before financial aid funds can be applied to students’ accounts. Therefore, attendance is recorded in the following ways:

- For in-person and blended-learning courses, students are required to attend the course by the 15th day of the semester (or equivalent for terms shorter than five weeks) to be considered attending. Students who have not met all attendance requirements for in-person and blended courses, as described herein, within the first two weeks or equivalent, will be considered not attending.
- For online courses, students are required to login at least two times per week and submit one assignment per week for the first two weeks of the semester, or equivalent to the 15th day of the term. Students who have not met all attendance requirements for online courses, as described herein, within the first two weeks or equivalent, will be considered not attending.

At the conclusion of the first two weeks of a semester or equivalent, instructors report any registered students who have “Never Attended” a course. Those students will be administratively withdrawn from that course. However, after the time period in the previous paragraphs, if a student stops attending a class or wants or needs to withdraw, for any reason, it is the student’s responsibility to take action to withdraw from the course. Students must complete and submit the appropriate Tri-C form by the established withdrawal deadline.

Tri-C is required to ensure that students receive financial aid only for courses that they attend and complete. Students reported for not attending at least one of their registered courses will have all financial aid funds held until confirmation of attendance in registered courses has been verified. Students who fail to complete at least one course may be required to repay all or a portion of their federal financial aid funds and may be ineligible to receive future federal financial aid awards. Students who withdraw from classes prior to completing more than 60 percent of their enrolled class time may be subject to the required federal refund policy.

Students having problems with coursework due to a prolonged absence should confer with the instructor or a counselor.

IV. LEARNING OUTCOMES ASSESSMENT

Occasionally, in addition to submitting assignments to their instructors for evaluation and a grade, students will also be asked to submit completed assignments, called ‘artifacts,’ for assessment of course and program outcomes and the College’s Essential Learning Outcomes (ELOs). The artifacts will be submitted in Blackboard or a similar technology. The level of mastery of the outcome demonstrated by the artifact DOES NOT affect the student’s grade or academic record in any way. However, some instructors require that students submit their artifact before receiving their final grade. Some artifacts will be randomly selected for assessment, which will help determine improvements and support needed to further student success. If you have any questions, please feel free to speak with your instructor or contact the Learning Outcomes Assessment office.

V. CONCEALED CARRY STATEMENT

College policy prohibits the possession of weapons on college property by students, faculty and staff, unless specifically approved in advance as a job-related requirement (i.e., Tri-C campus police officers) or, in accordance with Ohio law, secured in a parked vehicle in a designated parking area only by an individual in possession of a valid conceal carry permit.

As a Tri-C student, your behavior on campus must comply with the student code of conduct which is available on page 29 within the Tri-C student handbook, available at http://www.tri-c.edu/student-resources/documents/studenthandbook.pdf You must also comply with the College’s Zero Tolerance for Violence on College Property available at http://www.tri-c.edu/policies-and-procedures/documents/3354-1-20-10-zero-tolerance-for-violence-policy.pdf

VI. CORONAVIRUS/COVID-19 STATEMENT

Students are responsible for adhering to all College health and safety guidance, including that which relates to the COVID-19 pandemic.

Public health requirements and standards are changing rapidly, and the College is adapting its guidance accordingly. Please check your Tri-C email and visit tri-c.edu/coronavirus regularly for updates.
All students must adhere to the following general guidelines, until further notice:
• Remain at home if you are ill or experiencing symptoms of illness. Do not attend any in-person class or gathering.
• Notify your instructor(s) if you are ill, have tested positive for COVID-19, or were exposed to an individual who has tested positive for COVID-19 and they will report the information to the Tri-C Compliance & Risk Management team and you may be contacted for follow-up information.
• Wear a mask or face covering at all times, including, but not limited to: upon entering and exiting any Tri-C facility, in class, and in all common areas.
• Maintain a distance of at least six feet between yourself and others at all times and if you must pass near an individual do it quickly and do not linger.
• Provide the College with relevant information about your current health status and participate in any required on-site checks (e.g., temperature checks, current contact information, symptom profile, etc.).
• Use only designated areas of Tri-C facilities, including entrances and exits. Sign in and out of Tri-C facilities as directed.

The general guidelines listed above do not encompass all coronavirus-related guidance. These guidelines are subject to change at the discretion of the College and under the direction of public health authorities. Students who fail to adhere to this guidance may be subject to disciplinary action under the College’s Student Code of Conduct and the Student Judicial Code.

Outcomes
Course Outcome(s):
Implement and administer Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) and the network traffic these systems collect.

Objective(s):
2. Setup and administer an IDS in a working network.
3. Identify false positives and false negatives.
4. Demonstrate appropriate and ethical behavior and good work habits.

Course Outcome(s):
Analyze various attack signatures used to compromise computer systems.

Objective(s):
1. Setup and administer an IDS in a working network.
2. Dissect and analyze various types of normal and unusual traffic.
3. Identify false positives and false negatives.

Methods of Evaluation:
Evaluation can include any combination of the following:
1. Assignments
2. Quizzes
3. Exams
4. Lab Assignments
5. Projects
6. Reports
7. Oral Evaluations

Course Content Outline:
1. Introduction to Network Security Monitoring
   a. Understanding the concept of Defense-in-Depth
   b. Introduction to intrusion detection and prevention
2. Network and Host-Based Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
   a. Description of host-based IDS/IPS systems
   b. Description of network-based IDS/IPS systems
3. Fundamentals of Traffic Analysis
   a. The TCP/IP suite
   b. Dissecting a network packet
4. Advanced Traffic Analysis
   a. Packet sniffing
   b. Tcpdump basics
   c. Examining tcpdump output
5. Working with Filters/Rules for Network Monitoring
   a. Downloading and/or creating network monitoring filters/rules
   b. Managing network monitoring filters/rules
   c. Filter/rule execution
   d. Analyzing and Deconstructing Attack Signatures

Resources
