

**Digital Information & Technology Center of Excellence**

**Computer Systems Networking Department** (Cybersecurity, Linux, Microsoft, Cisco, BCIS)

# ITSY 2330: Intrusion Detection | HCC Online | #29053

Fall 2020 | 8 weeks (10.19.2020-12.13.2020)

3 Credit Hours | 98 hours per semester

## Instructor Contact Information

|  |  |  |
| --- | --- | --- |
| Instructor: Yaritza Garcia-Rivera | Office Phone: | N/A |
| Office: Online/Skype for Business | Office Hours: | When available |
| HCC Email: [yaritza.garciarivera@hccs.edu](mailto:yaritza.garciarivera@hccs.edu) | Office Location: | Skype for Business |

As your instructor, I am here to support you. Please feel free to schedule an appointment with me and discuss any problems that you are experiencing in this course or any other courses. Your performance in my class is very important to me.

### Instructor’s Preferred Method of Contact

I will respond within 48 hours or less during the week and in most cases during weekends. My preferred method is via canvas inbox message.

## What’s Exciting About This Course

What’s exciting about this course is that it is about Intrusion Detection! Intruders come in different forms and shapes (physical and virtual). This includes in phones, tablets, personal computers, as well as in servers and more. We will work together and use different methods of finding and maybe even blocking those intruders.

## My Personal Welcome

Welcome to this edition of Intrusion Detection – I’ve been expecting you! I, Yaritza Garcia, will be your instructor for this fall 2020 Intrusion Detection course. The main method of communication that I will use is Canvas. Please be sure to follow the syllabus as a reference for any important dates, to plan for the semester, and to review HCC policies. The best way to really discuss issues is via Canvas inbox. My goal is for you to learn skills that you can enhance further by tying in more networking, security, and programming.

## Prerequisites and/or Co-Requisites

ITSY 2330 requires college-level reading and writing skills. Research indicates that you are most likely to succeed if you have already taken and passed ENGL 1307. The minimum

requirements for enrollment in ITSY 2330 include ITSC 1307, ITMT 1358, ITNW 1425 or ITCC 1414, ITSY 1342. If you have enrolled in this course having satisfied these prerequisites, you have a higher chance of success than students who have not done so. Please carefully read and consider the repeater policy in the [HCCS Student Handbook.](http://www.hccs.edu/resources-for/current-students/student-handbook/)

## Canvas Learning Management System

This section of ITSY 2330 will use Canvas ([https://eagleonline.hccs.edu](https://eagleonline.hccs.edu/)) to supplement in- class assignments, exams, and activities. Please follow all the modules on Canvas and be

sure to start with the first module titled “Getting started.” You will use Canvas to access all the course material including class notes, exam reviews, videos, labs, and so on. You do not need to purchase anything for this course. You will also use Canvas to take your Midterm and Final exams (will be held in person).

HCCS Open Lab locations may be used to access the Internet and Canvas. **USE** [**FIREFOX**](https://www.mozilla.org/en-US/firefox/new/) **OR** [**CHROME**](https://www.google.com/chrome/browser/desktop/index.html) **AS THE INTERNET BROWSER**.

### HCC Online Information and Policies

Here is the link to information about HCC Online classes including the required Online Orientation for all fully online classes: <http://www.hccs.edu/online/>

### Scoring Rubrics, Sample Assignments, etc.

The scoring rubric is: Exam: 30%

Quizzes: 30%

Project: 25%

Attendance/Participation: 15%

# Instructional Materials

There is no required textbook for this course. You will receive all of the notes (via Word documents and Canvas discussions) and lectures. You will also have access to the VMware Academy as you will need it to retrieve the VMware Workstation (Windows) or VMware Fusion (Mac) in order to power Virtual Machines running Linux. We will be using Centos 7, Kali Linux, Security Onion and more as the operating systems.

## Other Instructional Resources

You will also have access to the VMware Academy as you will need it to retrieve the VMware Workstation (Windows) or VMware Fusion (Mac) in order to power Virtual Machines running Linux. We will be using Centos 7, Kali Linux, Security Onion and more as the operating systems.

### Tutoring

HCC provides free, confidential, and convenient academic support, including writing critiques, to HCC students in an online environment and on campus. Tutoring is provided by HCC personnel in order to ensure that it is contextual and appropriate. Visit the [HCC Tutoring](http://www.hccs.edu/resources-for/current-students/tutoring/) [Services](http://www.hccs.edu/resources-for/current-students/tutoring/) website for services provided.

### Libraries

The HCC Library System consists of 9 libraries and 6 Electronic Resource Centers (ERCs) that are inviting places to study and collaborate on projects. Librarians are available both at the libraries and online to show you how to locate and use the resources you need. The libraries maintain a large selection of electronic resources as well as collections of books, magazines, newspapers, and audiovisual materials. The portal to all libraries’ resources and services is the HCCS library web page at [http://library.hccs.edu](http://library.hccs.edu/).

### Supplementary Instruction

Supplemental Instruction is an academic enrichment and support program that uses peer- assisted study sessions to improve student retention and success in historically difficult courses. Peer Support is provided by students who have already succeeded in completion of the specified course, and who earned a grade of A or B. Find details at <http://www.hccs.edu/resources-for/current-students/supplemental-instruction/>.

# Course Overview

Computer information systems security monitoring, intrusion detection, and crisis management. Includes alarm management, signature configuration, sensor configuration, and troubleshooting components. Emphasizes identifying, resolving, and documenting network crisis and activating the response team.

## Core Curriculum Objectives (CCOs)

ITSY 2330 satisfies the computer science requirement in the HCCS core curriculum. The HCCS Computer Systems Networking Discipline Committee has specified that the course address the following core objectives:

* ***Critical Thinking***: Students will demonstrate the ability to engage in inquiry and analysis, evaluation and synthesis of information, and creative thinking by completing a written assignment such as a book report, research paper, or essay.
* ***Communication Skills***: Students will demonstrate effective development, interpretation and expression of ideas through written, oral, and visual communication by completing a written assignment such as a book report, research paper, or essay.
* ***Quantitative and Empirical Literacy***: Students will demonstrate the ability to draw conclusions based on the systematic analysis of topics using observation, experiment, and/or numerical skills by completing textbook reading assignments, completing assignments, and answering questions on quizzes and exams that pertain to Course Student Learning Outcome #2 below.
* ***Social Responsibility***: Students will demonstrate cultural self-awareness, intercultural competency, civil knowledge, and the ability to engage effectively in regional, national, and global communities by completing textbook reading assignments, completing assignments, and answering questions on quizzes and exams that pertain to Course Student Learning Outcome #4 below.
* ***Personal Responsibility (PR)***: To include the ability to connect choices, actions and consequences to ethical decision-making.

## Program Student Learning Outcomes (PSLOs)

Can be found at:

[https://www.hccs.edu/programs/areas-of-study/science-technology-engineering--](https://www.hccs.edu/programs/areas-of-study/science-technology-engineering--math/computer-systems-networking--telecommunications/) [math/computer-systems-networking--telecommunications/](https://www.hccs.edu/programs/areas-of-study/science-technology-engineering--math/computer-systems-networking--telecommunications/)

## Course Student Learning Outcomes (CSLOs)

Upon completion of ITSY 2330, the student will be able to:

1. Build IDS sensors and attach them to the network (hardware and software)
2. Install and manage a secure communication link between all sensors and the monitor
3. Install and manage event database(s)
4. Analyze an event and trends
5. Install, manage, and interpret syslog servers and system logs
6. Identify legal and policy issues associated with system and network monitoring
7. Deploy, implement, and test IDS security plan

## Learning Objectives

Learning Objectives for each CSLO are mapped to each module on Canvas:

1. Build IDS sensors and attach them to the network (hardware and software)
2. Install and manage a secure communication link between all sensors and the monitor
3. Install and manage event database(s)
4. Analyze an event and trends
5. Install, manage, and interpret syslog servers and system logs
6. Identify legal and policy issues associated with system and network monitoring
7. Deploy, implement, and test IDS security plan

# Student Success

There are 12 chapters, discussions, a midterm, a final, and a project. It will be up to you to be on top of your work every week. Please do not procrastinate! Intrusion Detection will be very useful to you if you plan on getting into the cybersecurity field, so why not pay close attention now and enjoy learning? I would expect that you spend a few hours every week. This course is meant to be a baseline to explore further. Successful completion of this course requires a combination of the following:

* Reading the notes
* Watching the videos
* Completing assignments
* Participating in the discussions
* Being punctual

There is no short cut for success in this course; it requires reading (and probably re-reading) and studying the material using the course objectives as a guide. It will also require you to try all the commands introduced to you many times as repetition is your best ally to learn and use some Linux commands. The more you use them, the more you realize how efficient it is to navigate through the Linux command line and be productive in finding information.

## Instructor and Student Responsibilities

As your Instructor, it is my responsibility to**:**

* Provide the grading scale and detailed grading formula explaining how student grades are to be derived
* Facilitate an effective learning environment through learner-centered instructional techniques
* Provide a description of any special projects or assignments
* Inform students of policies such as attendance, withdrawal, tardiness, and making up assignments
* Provide the course outline and class calendar that will include a description of any special projects or assignments
* Arrange to meet with individual students before and after class as required

As a student, it is your responsibility to**:**

* Attend class in person and/or online
* Participate actively by reviewing course material, interacting with classmates, and responding promptly in your communication with me
* Read and comprehend the textbook
* Complete the required assignments and exams
* Ask for help when there is a question or problem
* Keep copies of all paperwork, including this syllabus, handouts, and all assignments
* Attain a raw score of at least 50% on the departmental final exam
* Be aware of and comply with academic honesty policies in the [HCCS Student Handbook](http://www.hccs.edu/resources-for/current-students/student-handbook/)

# Assignments, Exams, and Activities

## Written Assignment

There is a project that is worth 40% of your final grade. The assignment will be checked for plagiarism so please do not try to copy and paste. If you do copy material, then be sure to reference the website.

## Exams

You will have two exams: a midterm and a final. They are both 50+ questions. The Midterm exam has many short-answer questions, multiple-choice, and true-false. The Final exam is all multiple-choice. You will receive reviews and jeopardy games as study material. Both exams will be taken in person. You will take them on Canvas.

## Grading Formula

I utilize a percentage-based points grading system. I group the Midterm and Final exam into a 30% exam group grade. I also add a third exam that I name “the best between the Midterm and Final” where I double the best grade between the Midterm & Final and I make an average of the three scores.

|  |  |
| --- | --- |
| Midterm Exam | 15% |
| Final Exam | 15% |
| Project | 40% |
| Attendance/Participation | 30% |

|  |  |
| --- | --- |
| **Grade** | **Total Points** |
| A | 90+ |
| B | 80+ |
| C | 70+ |
| D | 60+ |
| F | <60 |

### Incomplete Policy:

In order to receive a grade of Incomplete (“I”), a student must have completed at least 85% of the work in the course. In all cases, the instructor reserves the right to decline a student’s request to receive a grade of Incomplete.

**HCC Grading Scale can be found on this site under Academic Information:** [**http://www.hccs.edu/resources-for/current-students/student-handbook/**](http://www.hccs.edu/resources-for/current-students/student-handbook/)

# Course Calendar

|  |  |  |
| --- | --- | --- |
| **Week** | **Dates** | **Topics** |
| 1 | Oct 24 | Course intro Students’ intro  Introduction to Intrusion Detection |
| 2 | Oct 31 | Hacking Case Discussion IP Addressing Overview  Network and Computer attacks Social Engineering  Lab -Social Engineering Practice  Lab – VMWare, Install Kali Linux, Metasploitable, and Cent OS Quiz |
| 3 | Nov 7 | Hacking Case Discussion  Importance of programming on cybersecurity List of Tools  Lab cont.– VMWare, Install Kali Linux, Metasploitable, and CentOS Midterm Review |
| 4 | Nov 14 | Midterm Exam |
| 5 | Nov 21 | Hacking Case Discussion Projects  What is a SIEM? IDS/IPS Overview  Lab - Snort and Splunk Installation |
| - | Nov 28 | Thanksgiving Break |
| 6 | Dec 5 | Hacking Case Discussion Projects  Port Scanning Overview SANS Overview Wireshark Overview Final Exam Review  \*Lab – SANS Registration  \*Lab – Install Wireshark Quiz |
| 7 | Dec 12 | Cryptography & Network Attacks Embedded OS  Cont. Final Exam Review |
| 8 | Dec TBD | Final Exam  Bonus - Cybersecurity Related Certification (upload) |

## Syllabus Modifications

The instructor reserves the right to modify the syllabus at any time during the semester and will promptly notify students in writing, typically by e-mail, of any such changes.

# Instructor’s Practices and Procedures

## Missed Assignments

I do my best to accommodate your schedule and personal issues. I do not accept late submissions. I may accept an exam make-up with ample notification and untestable claim for missing the exam. A make-up exam is not a retake. That is, make-up exams are allowed only for missed exams.

## Academic Integrity

Academic integrity is important to me and note that I will report any student that cheats during an exam. I give students a chance to redo their projects should it have too much content that is plagiarized. Scholastic Dishonesty will result in a referral to the Dean of Student Services. See the link below for details.

Here’s the link to the HCC information about academic integrity (Scholastic Dishonesty and Violation of Academic Scholastic Dishonesty and Grievance):

[http://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-](http://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-procedures/) [procedures/](http://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-procedures/)

## Attendance Procedures

I will use Canvas course participation analytics and my own judgement to give a participation grade of up to 30%. I expect that you login to Eagle Online (Canvas) at least once a week and that you regularly follow the due dates of your assignments. This course is hybrid (online and in person). You need to attend in person for class and for your midterm & final exams.

## Student Conduct

I expect you to read and study the course material in a timely fashion. You are expected to check your email regularly. You are expected to practice the commands and not just retain theory. You are expected to have fun. You are required to respect and help your peers.

Cheating will not be allowed and tolerated.

# HCC Policies

Here’s the link to the HCC Student Handbook [http://www.hccs.edu/resources-for/current-](http://www.hccs.edu/resources-for/current-students/student-handbook/) [students/student-handbook/](http://www.hccs.edu/resources-for/current-students/student-handbook/) In it you will find information about the following:

* Academic Information
* Academic Support
* Attendance, Repeating Courses, and Withdrawal
* Career Planning and Job Search
* Childcare
* disAbility Support Services
* Electronic Devices
* Equal Educational Opportunity
* Financial Aid TV (FATV)
* General Student Complaints
* Grade of FX
* Incomplete Grades
* International Student Services
* Health Awareness
* Libraries/Bookstore
* Police Services & Campus Safety
* Student Life at HCC
* Student Rights and Responsibilities
* Student Services
* Testing
* Transfer Planning
* Veteran Services

## EGLS3

The EGLS3 ([Evaluation for Greater Learning Student Survey System](http://www.hccs.edu/resources-for/current-students/egls3-evaluate-your-professors/)) will be available for most courses near the end of the term until finals start. This brief survey will give invaluable information to your faculty about their teaching. Results are anonymous and will be available to faculty and division chairs after the end of the term. EGLS3 surveys are only available for the Fall and Spring semesters. EGLS3 surveys are not offered during the Summer semester due to logistical constraints.

<http://www.hccs.edu/resources-for/current-students/egls3-evaluate-your-professors/>

**Campus Carry Link** Here’s the link to the HCC information about Campus Carry: <http://www.hccs.edu/departments/police/campus-carry/>

## HCC Email Policy

When communicating via email, HCC requires students to communicate only through the HCC email system to protect your privacy. If you have not activated your HCC student email account, you can go [to HCC Eagle ID](http://www.hccs.edu/resources-for/current-students/student-e-maileagle-id/) and activate it now. You may also use Canvas Inbox to communicate.

## Housing and Food Assistance for Students

Any student who faces challenges securing their foods or housing and believes this may affect their performance in the course is urged to contact the Dean of Students at their college for support. Furthermore, please notify the professor if you are comfortable in doing so.

This will enable HCC to provide any resources that HCC may possess.

# Office of Institutional Equity

Use the link below to access the HCC Office of Institutional Equity, Inclusion, and Engagement (<http://www.hccs.edu/departments/institutional-equity/>)

## disAbility Services

HCC strives to make all learning experiences as accessible as possible. If you anticipate or experience academic barriers based on your disability (including long and short term conditions, mental health, chronic or temporary medical conditions), please meet with a

campus Abilities Counselor as soon as possible in order to establish reasonable accommodations. Reasonable accommodations are established through an interactive process between you, your instructor(s) and Ability Services. It is the policy and practice of HCC to create inclusive and accessible learning environments consistent with federal and state law. For more information, please go to [http://www.hccs.edu/support-](http://www.hccs.edu/support-services/disability-services/) [services/disability-services/](http://www.hccs.edu/support-services/disability-services/)

## Title IX

Houston Community College is committed to cultivating an environment free from inappropriate conduct of a sexual or gender-based nature including sex discrimination, sexual assault, sexual harassment, and sexual violence. Sex discrimination includes all forms of sexual and gender-based misconduct and violates an individual’s fundamental rights and personal dignity. Title IX prohibits discrimination on the basis of sex-including pregnancy and parental status in educational programs and activities. If you require an accommodation due to pregnancy please contact an Abilities Services Counselor. The Director of EEO/Compliance is designated as the Title IX Coordinator and Section 504 Coordinator. All inquiries concerning HCC policies, compliance with applicable laws, statutes, and regulations (such as Title VI, Title IX, and Section 504), and complaints may be directed to:

David Cross

Director EEO/Compliance

Office of Institutional Equity & Diversity 3100 Main

(713) 718-8271

Houston, TX 77266-7517 or [Institutional.Equity@hccs.edu](mailto:Institutional.Equity@hccs.edu) <http://www.hccs.edu/departments/institutional-equity/title-ix-know-your-rights/>

## Office of the Dean of Students

Contact the office of the Dean of Students to seek assistance in determining the correct complaint procedure to follow or to identify the appropriate academic dean or supervisor for informal resolution of complaints.

[https://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-](https://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-complaints/speak-with-the-dean-of-students/) [complaints/speak-with-the-dean-of-students/](https://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-complaints/speak-with-the-dean-of-students/)

## Department Chair Contact Information

Fidelis Ngang, [fidelis.ngang@hccs.edu.](mailto:fidelis.ngang@hccs.edu) 713-718-5552. Naseem Nikooei, [Naseem.nikooei@hccs.edu](mailto:Naseem.nikooei@hccs.edu). 713-718-7631.