Hudson County Community College

MATH, SCIENCE & TECHNOLOGY DIVISION

Course Title: Cyber Security. **Course Number**: **CSC 232** **Credits:3**
INSTRUCTOR:
OFFICE HOURS: TBD **EMAIL ADDRESS**:

PHONE: **LOCATION**:

Course Outline and description:
Topics include but not limited:

This course is designed as a core major requirement for students majoring in Computer Science - Cyber Security Option, or as an elective course for students majoring in Computer Science Option. In this course, students will learn and understand threats, risks and challenges facing the cyber world. Students will learn different techniques to make the computing environment and crucial data safer and more secure. Students will be able to realize the impact of security breaches caused by malware, counterfeit software, viruses and worms.
This course covers all security topics considered Core Computer Science Curriculum. Learned knowledge can be used to prep for CISSP Certification, and includes in-depth coverage of Computer Security, Technology and Principles, Software Security, Management Issues, Cryptographic Algorithms, Internet Security and more.

Objective:

Upon successful course completion, students will be able to:

1. **Demonstrate the understanding** of a variety of computer security techniques, security polices, computer network security principals, technical documents regarding information hiding techniques, challenges and risks in securing the computing environments.
2. **Apply** the use of filters to protect assets – Routers, Firewalls, Demilitarized Zones (DMZ), and perform security awareness.
3. **Interpret** the overall needs, risks threats and challenges to the cyber world and to digital data.
4. **Apply** different types of encryption techniques needed to secure digital data.
5. **Perform** watermarking of digital images using MATLAB.
6. **Perform** risk analysis and resources management required for securing crucial data.
7. **Demonstrate the understanding of Biometric techniques** – Fingerprinting, Vascular Patterns, Thermal Scans, Retinal Scans, etc.

Evaluation Criteria

- Student will be graded based on:

- Exam 1 (Lecture) 15%
- Midterm Exam (Lecture) 20%
- Research Article Presentation: 20% (Rubric Attached)
- Homework assignments and collaboration work(**labs**): 20%
- Final exam (Lecture) 25%

Grading Policy:

95 to 100 A	90 to 94 A-	85 to 89 B+	80 to 84 B
75 to 79 B-	70 to 74 C+	65 to 69 C	64 to 0 F

** Excess of absence will result in a failing grade!! (3 Absences maximum).
** 20 minutes of lateness is considered one absence.
There will be no makeup for missing tests.
Any student misses a class for any reason is responsible for the notes and assignments given on the day he/she missed.

Academic Integrity Standards:

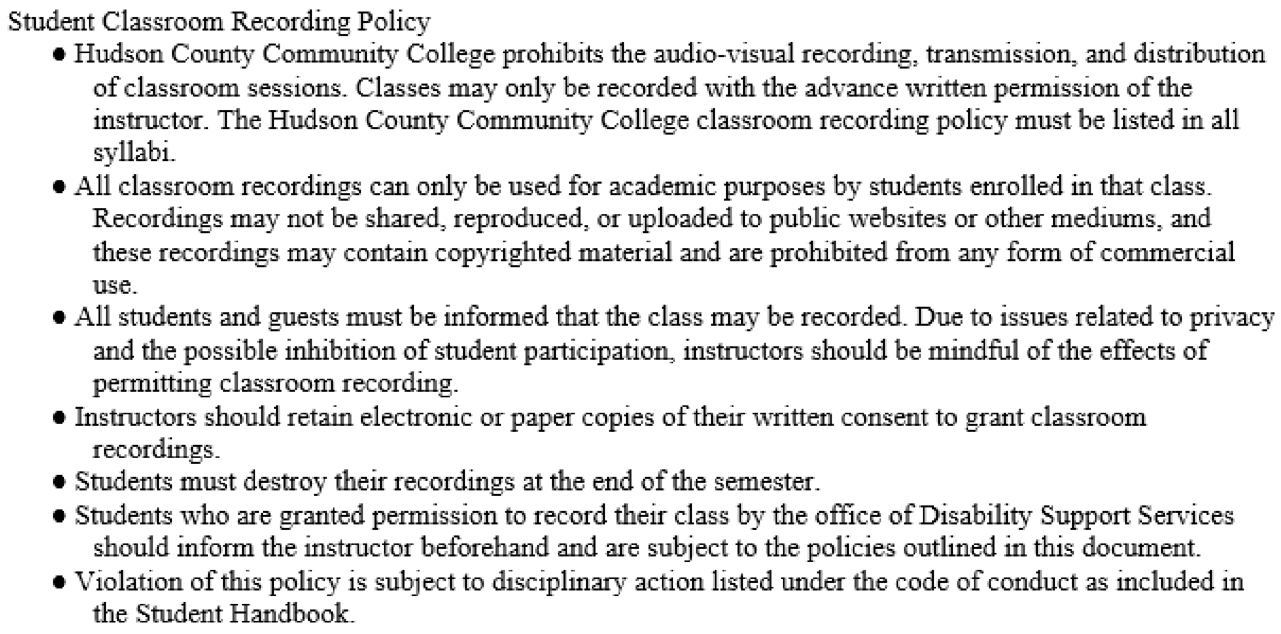
Academic integrity is central to the pursuit of education. For students at HCCC this means maintaining the highest ethical standards in completing their academic work.
Violations of the principle of academic integrity include:
Cheating on exams.
Reporting false research data or experimental results.
Allowing other students to copy one's work to submit to instructor.
Communicating the content of an exam to other students who will be taking the same test.
Submitting the same project in more than one course, without discussing this first with the instructor.
Submitting plagiarized work. Plagiarism is the use on another writer's words or ideas without properly crediting that person. This unacknowledged use may be from published books or articles, or another student's work.

Disability Support Services:

Students with disabilities who believe that they might need accommodations in the class are encouraged to contact the Counselor/coordinator, disability Support services at 201-360-4157.

Required Textbook:

Computer Security – Principles AND Practice
3rd Edition William Stallings and Lawrie Brown
Amazing Computer Security
Threats/ vulnerability/ counter measure approaches
Charles P. Pfleeger and Shari Lawrence Pfleeger
ISBN-13: 978-0-13-377392-7
ISBN-10 0-13-377392-2



Student Classroom Recording Policy

- Hudson County Community College prohibits the audio-visual recording, transmission, and distribution of classroom sessions. Classes may only be recorded with the advance written permission of the instructor. The Hudson County Community College classroom recording policy must be listed in all syllabi.
- All classroom recordings can only be used for academic purposes by students enrolled in that class. Recordings may not be shared, reproduced, or uploaded to public websites or other mediums, and these recordings may contain copyrighted material and are prohibited from any form of commercial use.
- All students and guests must be informed that the class may be recorded. Due to issues related to privacy and the possible inhibition of student participation, instructors should be mindful of the effects of permitting classroom recording.
- Instructors should retain electronic or paper copies of their written consent to grant classroom recordings.
- Students must destroy their recordings at the end of the semester.
- Students who are granted permission to record their class by the office of Disability Support Services should inform the instructor beforehand and are subject to the policies outlined in this document.
- Violation of this policy is subject to disciplinary action listed under the code of conduct as included in the Student Handbook.

Detailed outline of suggested topics.

Day	Content
1	Syl, and introduction
2	Computer Security concepts Threats, Attacks, and Assets Security Functional Requirements Fundamental Security Design Principles Attack Surfaces and Attack Trees Computer Security Strategy
3	Cryptographic Tools Message Authentication and Hash Functions Public-Key Encryption Digital Signatures and Key Management Random and Pseudorandom Numbers Practical Application: Encryption of Stored Data Confidentiality with Symmetric Encryption
4	User Authentication Electronic User Authentication Principles Password-Based Authentication Token-Based Authentication Biometric Authentication Remote User Authentication Security Issues for User authentication Practical Application: An Iris Biometric System

5	Test 1 (ch1, 2, 3) Access Control Principles Subjects, Objects, and Access Rights Discretionary Access Control Example: UNIX File Access Control Role-Based Access Control Attribute-Based Access Control Identity, Credential, and Access Management Trust Frameworks
6	Database and Cloud Security The Need for Database Security Database Management Systems SQL Injection Attacks Database Access Control Inference, Database Encryption Cloud Computing, Cloud Security Risks and countermeasures Data Protection in the Cloud, Cloud Security as a Service, Malicious Software Advanced Persistent Threat propagation – Infected Content - Viruses
7	Propagation – Vulnerability Exploit – Worms, Propagation – Social Engineering – SPAM E- Mail, Trojans Payload – System Corruption Payload – Attack Agent – Zombie, Bots Payload – Information Theft – Keyloggers, Phishing, Spyware
8	Mid Term Exam (ch 1, 2, 3, 4, 5)
9	Payload – Stealthing – Backdoors, Rootkits Denial-of-Service Attacks Flooding Attacks Distributed Denial-of-Service Attacks Application-Based Bandwidth Attacks Defenses Against Denial-of-Service Attacks Selecting/identifying topic, faculty to help students in selecting and shaping up their topics (see topic examples below the table)
10	Intrusion Detection Analysis Approaches Host-Based Intrusion Detection Network-Based Intrusion Detection Distributed or Hybrid Intrusion Detection Intrusion Detection Exchange Format Honeypots, Example System: Snort

11	Firewalls and Intrusion Prevention Systems The Need for Firewalls Firewall Characteristics and Access Policy Types of Firewalls Firewall Basing Firewall Location and Configurations Intrusion Prevention Systems Example: Unified Threat Management
12	Software Security Software Security Issues Handling Program Input Writing Safe Program Code Interacting with the OS and Other programs Handling Program Input
13	Introduction to Operating System Security System Security Planning Operating Systems Hardening Application Security Security Maintenance Linux/UNIX /Windows Security Virtualization Security
14	Project presentation
15	Review and Final Exam

Cyber Security labs (		Course
1	Securing the pfSense Firewall	CSC-232
2	Implementing NAT and Allowing Remote Access	CSC-232
3	Implementing Common Protocols and Services	CSC-232
4	Examining Wireless Networks	CSC-232
5	Implementing Security Policies on Windows and Linux	CSC-232
6	Data Backups in Windows, BSD, and Linux	CSC-232
7	Incident Response Procedures, Forensics, and Forensic Analysis	CSC-232
8	Crafting and Deploying Malware	CSC-232

9	Social Engineering	CSC-232
10	Exploiting Wireless Security	CSC-232
11	Deep Dive in Packet Analysis - Using Wireshark and Network Miner	CSC-232
12	Vulnerability Scanners and Penetration Testing	CSC-232
13	Patching, Securing Systems, and Configuring Anti-Virus	CSC-232
14	Using Active Directory in the Enterprise	CSC-232
15	Securing Data Using Encryption on a Windows System	CSC-232

** Homework and group collaboration: after each session students, will be assigned homework and groupwork from a selection of end of chapter Questions and Problems.

*** Project Topics examples:
Develop a detailed Security policy for a certain business or agency.
Plan a disaster recovery procedure.
Set up an incident response team and process.
Cryptography and Steganography