CLEVELAND INSTITUTE OF ELECTRONICS SYLLABUS

Course Number: S360

Course Name: Computer Security

Course Clock Hours: 90

Course Prerequisites: None

Course Co-requisites: None

Course Contact Information: www.cie-wc.edu faculty@cie-wc.edu
1-800-243-6446 (216) 781-9400 (216) 781-0331 (fax)

Course Description: This course is designed to be the gateway into the entire field of computer security. It brings together all of the basic concepts, terminology, and issues, along with the practical skills essential to security. It will cover core topics such as vulnerability assessment, virus attacks, buffer overflow, hacking, spyware, network defense, firewalls, VPNs, Intrusion Detection Systems, and passwords. Topics will also fully address more specialized issues, including cyber terrorism, industrial espionage and encryption - including public/private key systems, digital signatures, and certificates.

Course Objectives: Upon completion of this course the student will:

- Comprehend and analyze key attacks, including denial of service, malware, and viruses
- Discuss subject areas such as cyber terrorism, computer fraud, and industrial espionage
- Recommend and implement strategies, tools and policies to defend networks from outside attacks

Course Readings: The required readings will be drawn from the textbook Computer Security Fundamentals, 2nd Edition (ISBN 0-7897-4890-8). The author is Chuck Easttom and the publisher is Pearson. The study guide was written by Bruce Coscia. Students should complete the required readings and solve all problems in the exercise sections before continuing to the next topic.

Student Evaluation and Grading: There are fifteen lessons in this course. The lessons are broken into twelve exams and three projects. The twelve lessons conclude with an examination; all examinations are open book. The minimum passing score of 70% must be achieved but if the score is less than 70%, the lesson must be retaken to earn a passing score of 70% overall. The fifteen scores are averaged together and constitute 100% of the course grade.

93% - 100%	A	The final grade for this course will be determined as follows:
86% - 92.9%	B	12 examinations + 3 projects = 100%
78% - 85.9%	C	
70% - 77.9%	D	

Course Schedule: You should complete the following lessons in the order shown in the table. It is best to complete 1-2 lessons per week to maintain your schedule.

Lesson Number	Title of Lesson	Topics Covered
3601C	Introduction to Computer Security	• Identify threats to a computer network: intrusion, denial-of-service attacks, and malware, and whether to take perimeter and/or layered approaches to network security. • Use online resources to secure your network.
3602C	Networks and the Internet	• Identify each of the major protocols used in network communication. • Explain the use of firewalls and proxy servers.
3603C	Cyber-stalking, Fraud and Abuse	• Understand the following: Internet investment scams, auction frauds, identity theft, cyber stalking. • Know what laws apply to these computer crimes.
3604C	Denial-of-Service Attacks	• Understand how denial-of-service (DoS) attacks are accomplished. • Know how to defend against specific DoS attacks.
3605C	Malware	• Understand viruses and Trojan horses and how they propagate, as well as a working knowledge of several specific virus outbreaks and Trojan horse attacks. • Defend against various attacks through sound practices, antivirus software, and anti-spyware software.
3606C	Project 1	• Case problems from preceding chapters
3607C	Techniques Used by Hackers	• Understand the basic methodology used by hackers and their mentality, as well as be familiar with some of the basic tools
3608C	Industrial Espionage in Cyberspace	• Know what is meant by industrial espionage and some of the methods used to attempt industrial espionage. • Know how to protect a system from espionage.
3609C	Encryption	• Explain and discuss the basics of encryption and modern cryptography methods. • Understand the function and protocols of VPNs.
3610C	Computer Security Software	• Choose the best type of firewall for an organization. • Employ intrusion detection systems to detect problems on your system.
3611C	Project 2	• Case problems from preceding chapters
3612C	Security Policies	• Recognize the importance of security policies • Evaluate and improve existing policies.
3613C	Network Scanning and Vulnerability Scanning	• Understand and be able to conduct basic system reconnaissance. • Use port monitoring utilities.
3614C	Cyber Terrorism and Information Warfare	• Understand and explain what cyber terrorism is and how it has been used in some actual cases. • Locate court and criminal records on the web.
3615C	Introduction to Forensics / Project 3	• Case problems from preceding chapters