Syllabus for IAS-5520

VULNERABILITIES, THREATS, AND ATTACKS

COURSE DESCRIPTION

The impact of a security breach can be devastating to any organization. Information technology (IT) practitioners must have the skills to identify and address system vulnerabilities including weaknesses related to hardware, software, interrelated systems, and personnel. In this course, students will explore current and potential threats to information assets and will develop a comprehensive awareness of prevailing trends in malicious attacks. This course will provide students with the skills and knowledge needed to secure organizational resources and to develop effective methods to detect and monitor internal and external malicious activity. Topics covered in this course include: passive and active attacks, technology audits, physical security, computer security policies, contingency planning, business impact analysis, password management, information warfare, intrusion detection, risk assessment and auditing, operational security, permissions and user rights, service patches, securing network services, and security baseline analyzers. Students will learn to identify threat vectors and to develop strategies for implementing a prioritized, risk-based approach to mitigating security.

COURSE TOPICS

- Malicious attack trends
- Passive and active attacks
- Threat vectors
- Cybersecurity countermeasures
- Operating system security
- Network security
- Cybersecurity management: policies and audits
- Risk management
- Contingency planning
- Cyber warfare

COURSE OBJECTIVES

After completing this course, you should be able to:

CO1 Prioritize asset values.

CO2 Evaluate threats.

CO3 Recommend cybersecurity countermeasures.

CO4 Evaluate hardware security at the system level.

CO5 Evaluate intrusion detection systems.

CO6 Assess laws applicable to cybersecurity.

CO7 Formulate cybersecurity business continuity plans.

CO8 Compare risk assessment techniques.

COURSE MATERIALS

You will need the following materials to complete your coursework. Some course materials may be free, open source, or available from other providers. You can access free or open-source materials by clicking the links provided below or in the module details documents. To purchase course materials, please visit the University's textbook supplier.

Required Textbook

- Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing*. Upper Saddle River, NJ: Pearson Education.
  ISBN-13: 978-0134085043

COURSE STRUCTURE

Vulnerabilities, Threats, and Attacks is a three-credit, online course consisting of five modules and a final project. Modules include an overview, topics, learning objectives, study materials, and activities. Module titles are listed below.

- **Module 1: Cybersecurity Threats**
  Course objectives covered in this module: CO1, CO2

- **Module 2: Cybersecurity Countermeasures**
  Course objectives covered in this module: CO3

- **Module 3: Hardware Security and Intrusion Detection Systems**
  Course objectives covered in this module: CO4, CO5

- **Module 4: Cybersecurity Laws and Business Continuity Plans**
  Course objectives covered in this module: CO6, CO7

- **Module 5: Risk Assessment Techniques**
  Course objectives covered in this module: CO8

ASSESSMENT METHODS

For your formal work in the course, you are required to participate in online discussion forums, complete written assignments, and complete a final project. See below for details.

Consult the Course Calendar for due dates.

Promoting Originality

One or more of your course activities may utilize a tool designed to promote original work and evaluate your submissions for plagiarism. More information about this tool is available in this document.

Discussion Forums

This course requires you to participate in ***five*** graded discussion forums. There is an ungraded but required Introductions Forum in Module 1.

Deadlines for posting discussion threads are given in the Course Calendar. For posting guidelines and additional help with discussion forums, please see the Online Student Handbook located within the General Information section of the course website.

Written Assignments

You are required to complete ***four*** written assignments. The written assignments are on a variety of topics associated with the course modules.

Final Project

Students will conduct a research project, the final product of which is a written paper. The purpose of the research is to do a risk analysis of all breaches discussed during this course, apply program level controls, and, by doing so, for the students to demonstrate their comprehension of the course material.

GRADING AND EVALUATION

Your grade in the course will be determined as follows:

- **Discussion forums (5)**—30%
- **Written assignments (4)**—36%
- **Final project**—34%

All activities will receive a numerical grade of 0–100. You will receive a score of 0 for any work not submitted. Your final grade in the course will be a letter grade. Letter grade equivalents for numerical grades are as follows:

A	=	93–100	B	=	83–87
A–	=	90–92	C	=	73–82
B+	=	88–89	F	=	Below 73

To receive credit for the course, you must earn a letter grade of C or higher on the weighted average of all assigned course work (e.g., assignments, discussion postings, projects). Graduate students must maintain a B average overall to remain in good academic standing.

STRATEGIES FOR SUCCESS

First Steps to Success

To succeed in this course, take the following first steps:

- Read carefully the entire Syllabus, making sure that all aspects of the course are clear to you and that you have all the materials required for the course.

- Take time to read the entire Online Student Handbook. The Handbook answers many questions about how to proceed through the course and how to get the most from your educational experience at Thomas Edison State University.

- Familiarize yourself with the learning management systems environment—how to navigate it and what the various course areas contain. If you know what to expect as you navigate the course, you can better pace yourself and complete the work on time.

- If you are not familiar with web-based learning be sure to review the processes for posting responses online and submitting assignments before class begins.

Study Tips

Consider the following study tips for success:

- To stay on track throughout the course, begin each week by consulting the Course Calendar. The Course Calendar provides an overview of the course and indicates due dates for submitting assignments, posting discussions, and the final project.

- Check Announcements regularly for new course information.

COMMITMENT TO DIVERSITY, EQUITY, AND INCLUSION

Thomas Edison State University recognizes, values, and relies upon the diversity of our community. We strive to provide equitable, inclusive learning experiences that embrace our students' backgrounds, identities, experiences, abilities, and expertise.

ACCESSIBILITY AND ACCOMMODATIONS

Thomas Edison State University recognizes disability as a facet of diversity and seeks to advance access to its educational offerings. Students with disabilities may seek accommodations by contacting the Office of Student Accessibility Services via email at ada@tesu.edu or phone at (609) 984-1141, ext. 3415. Individuals who are deaf or hard of hearing may call the TTY line at (609) 341-3109.

ACADEMIC POLICIES

To ensure success in all your academic endeavors and coursework at Thomas Edison State University, familiarize yourself with all administrative and academic policies including those related to academic integrity, course late submissions, course extensions, and grading policies.

For more, see:

- University-wide policies
- Undergraduate course policies and regulations
- Graduate academic policies
- Nursing student policies
- Academic code of conduct