Syllabus for CYB-4410—Network Forensics

COURSE DESCRIPTION

This course is a subcategory of digital forensics that focuses specifically on networks. It investigates networks from a digital forensics perspective and explores application of techniques used in forensic investigations to collect and analyze information from computer networks in response to network intrusions. The course includes analysis of network traffic, identification of threats and vulnerabilities, and evaluation of effects on the system.

COURSE TOPICS

- Capturing, storing, analyzing, and deciphering network activity
- Network forensic methodologies as related to incident response and investigation
- Network forensic capabilities to improve network performance
- Network forensic tools and their utility in identifying anomalous or malicious activity

COURSE OBJECTIVES

After completing this course, you should be able to:

CO 1 Describe potential system attacks and the actors who might perform them.

CO 2 Compare and contrast the resources and motivations of bad actors in cyberspace.

CO 3 Examine the architecture of a particular system in order to identify vulnerabilities and risks.

CO 4 Determine the appropriate measures to respond to a system compromise.

CO 5 Analyze common security failures.

CO 6 Track the packets involved in a simple TCP connection or a trace of such a connection.

CO 7 Use a network monitoring tool and network mapping tool to investigate a suspected compromise.

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

Johansen, G. (2022). *Digital forensics and incident response: Incident response tools and techniques for effective cyber threat response* (3rd ed.). Packt Publishing.
ISBN-13: 978-1803238678

Note About Infosec Learning Labs

In completing your coursework, you will be using Infosec Learning Labs, a virtual platform that contains interactive labs, which provide you with a real-world application and hands-on learning experience to practice various cybersecurity skills and concepts.

To access the labs, visit the Infosec section of the course website. When you click the Infosec Learning Labs link in your course for the first time, you will be redirected to an account setup page. You will be asked for some basic information to create your account and then make a payment. The price covers all labs needed for this course and access for 6 months.

COURSE STRUCTURE

Network Forensics is a three-credit, online course consisting of **six** modules. Modules include an overview, topics, learning objectives, study materials, and activities. Module titles are listed below.

- **Module 1: Introduction to Forensics**
  Course objectives covered in this module: CO 3, CO 4, CO 5

- **Module 2: Forensic Research**
  Course objectives covered in this module: CO 4, CO 5, CO 6, CO 7

- **Module 3: Packets**
  Course objectives covered in this module: CO 5, CO 6, CO 7

- **Module 4: Log Analysis**
  Course objectives covered in this module: CO 1, CO 3, CO 4

- **Module 5: Event Correlation**
  Course objectives covered in this module: CO 5, CO 7

- **Module 6: Forensic Challenges**
  Course objectives covered in this module: CO 1, CO 2, CO 4

ASSESSMENT METHODS

For your formal work in the course, you are required to participate in online discussion forums, complete written assignments, complete Infosec Learning Labs, 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

In addition to an ungraded Introductions Forum, you are required to participate in **six** graded online class discussions.

Communication with your mentor and among fellow students is a critical component of online learning. Participation in online class discussions involves two distinct activities: an initial response to a discussion question and at least two subsequent comments on classmates' responses.

All of these responses must be substantial. Meaningful participation is relevant to the content, adds value, and advances the discussion. Comments such as "I agree" and "ditto" are not considered value-adding participation. Therefore, when you agree or disagree with a classmate or your mentor, state and support your position.

You will be evaluated on the quality and quantity of your participation, including your use of relevant course information to support your point of view, and your awareness of and responses to the postings of your classmates. Remember, these are discussions: responses and comments should be properly proofread and edited, mature, and respectful.

Written Assignments

You are required to complete **three** written assignments. The written assignments are on a variety of topics associated with the course modules. For specific details, consult the individual course modules.

Infosec Learning Labs

You are required to complete and submit results for **five** Infosec Learning Labs for this course.

Each lab is either 90 minutes or 120 minutes in duration, regulated by a timer. They are designed to be completed in one sitting to simulate a real experience, so you cannot save your progress to return later. For an optimal experience, use a Chrome web browser with an Internet connection to run the labs.

While completing each lab, take a screenshot toward the end. Then, write a 250- to 300-word reflection (1 page) that describes your overall impressions and experience of completing the lab. Include what you found to be the most difficult steps of the lab, anything that surprised you throughout the process, what you learned, and how the lab specifically relates to the course topics. For an optimal experience, use a Chrome web browser with an Internet connection to run the labs. While completing each lab, take a screenshot of the performance report screen. **Submit both the screenshot and your lab reflection** to your mentor using the appropriate “Infosec Lab Results” link in Moodle. Your mentor will review your submissions and give you credit for each completed activity. Be sure to reference the Course Calendar for due dates.

Please see the Infosec Learning Labs section of the course website for further details and instructions. Consult the Course Calendar for due dates.

Final Project

You are required to complete a three-part final project, demonstrating technical skills learned as part of this course. During Part 1, you will use WireShark to obtain a packet capture (pcap) and import the results. Part 2 requires you to analyze the data and present your analysis. Part 3 requires you to reflect on what you learned in the course as well as what you learned when using Wireshark.

Be sure to visit the Final Project area of the course website for full requirements, details, and instructions for this project. Consult the Course Calendar for due dates.

GRADING AND EVALUATION

Your grade in the course will be determined as follows:

- **Online discussions (6)**—20%
- **Written assignments (3)**—30%
- **Infosec labs (5)**—20%
- **Final project (3 parts)**—30%
    - Part 1 (Lab Activity) (15%)
    - Part 2 (Analysis Presentation) (10%)
    - Part 3 (Written Reflection) (5%)

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	C+	= 78–79
A–	= 90–92	C	= 73–77
B+	= 88–89	C–	= 70–72
B	= 83–87	D	= 60–69
B–	= 80–82	F	= Below 60

To receive credit for the course, you must earn a letter grade of C or better (for an area of study course) or D or better (for a course not in your area of study), based on the weighted average of all assigned course work (e.g., exams, assignments, discussion postings).

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 submitting the final project.

- Check Announcements regularly for new course information.

Using AI Ethically: A Guide for TESU Students

TESU's Academic Code of Conduct permits student AI use in support of their writing and research process--not as a replacement for original writing. Document AI use with an acknowledgment statement at the end of each assignment, noting the tools and prompts used. Cite any AI-generated content on the References page. Please review Using AI Ethically: A Guide for TESU Students for more detailed 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 adheres to the Americans with Disabilities Act (ADA, 1990; ADAAA, 2008) and Section 504 of the Rehabilitation Act of 1973. The Office of Student Accessibility Services (OSAS) oversees requests for academic accommodations related to disabilities; a student who is pregnant, postpartum, or a student parenting a newborn who is not the birth parent [as covered under NJSA18A]; and students requesting academic accommodation for a short-term/temporary illness and/or injury. Information can be found on the Office of Student Accessibility Services webpage and questions can be sent to ADA@tesu.edu.

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 academic policies
- Undergraduate course policies
- Graduate academic policies
- Graduate course policies
- Nursing student policies

- Nursing graduate student policies
- International student policies
- Academic code of conduct