EEE 4752 Introduction to Network Forensics and Incident Response

Department of Electrical & Computer Engineering
Florida International University
Spring 2021

Classroom	**:**	Online
Class Time	**:**	NA
Faculty	**:**	Dr. Alexander Pons
Office Hours	**:**	M & W 10:30-12:00 am or by Appointment
Office	**:**	EC – 3145
Phone	**:**	305.348.7253
Email	**:**	aperezpo@fiu.edu
Prerequisite	**:**	EEL 2880 Applied Software Techniques in Engineering
Textbook		Ric Messier Network Forensics, 2nd Edition ISBN: 978-1-119-32828-5 Publisher: Wiley (2017)

Course Description

The course covers the theoretical and practical aspects of the foundations of computer network security, incident response tools and techniques, and an overview of how criminals are using computer networks to commit crime. This course will introduce students to the concept of "data in motion," how networks are used to transfer data, communication protocols, and challenges associated with the capture and interpretation of this data. This course will provide an overview of tools and techniques to capture and analyze network data.

Course Objectives

This course provides students the theoretical and fundamental concepts to perform and apply those concepts to a network environment. This course places a strong emphasis on digital forensic procedures, digital forensic tools, and legal issues relating to digital forensics in a network environment. This course uses advanced forensic tools and hands on exercises to emphasize the procedures that students will utilize in the field as forensic investigators.

Topics Covered

1. Network fundamentals
2. Different type of information obtain from networks
3. Incident response
4. Apply Wireshark to analysis network traffic flow
5. Identifying systems and a network
6. Router analysis
7. Log file analysis
8. Network security/encryption

9. Challenges associated in the capture and analysis of "data in motion"
10. Using the tools to effectively search, analyze and report on data discovery

ABET Relationship of course to program outcomes:
(Select corresponding boxes below to applicable program outcomes for the course.)

☒ 1. an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.

☒ 2. an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.

☒ 3. an ability to communicate effectively with a range of audiences.

☐ 4. an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.

☐ 5. an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.

☐ 6. an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions.

☒ 7. an ability to acquire and apply new knowledge as needed, using appropriate learning strategies.

Tentative Grading Scale

Grading Scale:		
A	**95-100**	**"Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook."**
A-	**90-94**	
B+	**86-89**	
B	**82-85**	
B-	**78-81**	
C+	**74-77**	
C	**70-73**	
D	**60-69**	
F	**< 59**	

Grading Scheme

Linkedin Learning Quizzes	**5%**
Weekly Quizzes	**10%**
Discussions	**15%**
Assignments	**25%**
Case Study	**5%**
Mid Exam	**20%**
Final Exam	**20%**
Total	**100%**

University's Code of Academic Integrity

Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational Mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook.
More information can be found at http://academic.fiu.edu/academic_misconduct.html

Department Regulations Concerning Incomplete Grades

To qualify for an Incomplete, a student:

1. Must contact (e.g., phone, email, etc.) the instructor or secretary before or during missed portion of class.
2. Must be passing the course prior to that part of the course that is not completed
3. Must make up the incomplete work through the instructor of the course
4. Must see the Instructor. All missed work must be finished before last two weeks of the next term.

University policies on sexual harassment, and religious holidays, and information on services for students with disabilities

Please visit the following websites:
http://academic.fiu.edu/
http://drc.fiu.edu

Course Policies

- **Exams:** will be conducted in class during the class time.
- **Quizzes** will be administered during class time.
- **Attendance:** Attendance in the course is **mandatory** and a student is not allowed to miss any class during the semester. There will be a **penalty** for missing classes and it may affect your final grade.
- **Academic Misconduct:** For work submitted, it is expected that each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- **Unexcused Absences:** Two unexcused absences are permitted during the term. More than two will result in the loss of points from your final grade. (1 point per absence above two, 3 points per absence above 5).
- **Excused Absences:** Only emergency medical situations or extenuating circumstances are excused with proper documentation. After reviewing documentation you are required to email a description of the excuse and absence dates as a written record to aperezpo@fiu.edu.
- **On Time:** As in the workplace, on time arrival and preparation are required. Two "lates" are equivalent to one absence. (Leaving class early is counted the same as tardy.)
- **Deadlines:** Assignments are due at the beginning of the class period on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- To get assistance try to see me by an appointment.
- Students are encouraged to ask questions and to discuss course topics with the instructor and with each other.

- **Any work submitted should display Panther ID number and should be signed, as the students' own work, and that no unauthorized help was obtained.**
- Cell phones, communicators, MP3 players, head sets are not allowed to be used in the class.
- **DO NOT** send assignments by email.
- Instructor reserves right to change course materials or dates as necessary.

Exam policy

1. Make sure to complete the assigned homework in order to do well in the exam.
2. All exams are closed book and closed notes.
3. Use of any electronic device with keyboard is prohibited. This also applies to cellphones with messaging system.
4. No discussion is permitted during the exams.
5. Instructor is not compelled to give credit for something he cannot read or follow logically.
6. Cheating is considered as a serious offense. Students who are caught will receive the appropriate consequences.

Class Schedule

Week	Date	Weekly Topic
1		Getting Started and Introduction
2		Network Forensics and Incident Response Basics
3		Networking Fundamentals I
4		Networking Fundamentals II
5		Search for Host-Artifacts
6		Packet Capture and Analysis
7		Attack Types
8		Location Awareness **Mid Term Exam**
9		How to Prepare for an Attack
10		Intrusion Detection Systems
11		Using Firewalls and Application Logs
12		Correlated Attacks
13		Network Scanning
14		Encryption and Cloud Computing **Final Exam**