Syllabus for CYB735 Network Forensics

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

This course covers protocol analysis, identification of malicious behavior in systems forensic investigations through event log aggregation, correlation and analysis. Students will analyze clips of network protocol analysis to discern methods of attacks and malicious activities. Reviews wired and wireless protocols and cover their associated attacks, with case studies involving protocol analysis, log analysis, and other tools.

Extended Course Description

The skill of protocol analysis can help protect networks via programming intrusion detection/prevention systems, identify malicious behavior in networks, and help in forensic investigations through event log aggregation, correlation and analysis. Students will analyze clips of network protocol analysis to discern methods of attacks and malicious activities. The course will review wired and wireless protocols and cover their associated attacks, with case studies involving protocol analysis, log analysis, and other tools.

Prerequisite(s)

CYB703 Network Security

Program Outcomes

This course addresses the following competencies and program outcomes of the Masters of Science in Cybersecurity:

- Program Outcome 2: Interpret and analyze network protocols
- Program Outcome 15: Identify and assess attacks through forensics
- Program Outcome 16: Interpret legal implications of security incidents and conduct investigations using industry best practices

Course Outcomes

Upon completing this course, you will be able to do the following:

1. Analyze clips of network protocol analysis to discern methods of attacks and malicious activities
2. Aggregate and correlate logs to discern methods of attacks and malicious activities
3. Discern how a product interfaces on the network in order to determine potential security risks
4. Recognize regulation applicable to network forensics according to the Computer Fraud and Abuse Act

Course Requirements/Components

Labs and Exercises

The labs provide you hands on experience with the course concepts. Generally, there is one lab or exercise for each module. There will be many labs held in the Virtual lab.

Quizzes

Each topic will include quizzes that enable students to practice with vocabulary, concepts and protocol analysis problems.

Protocol Project and Presentation

It is impossible to analyze network transmissions if you do not have a thorough understanding of protocols. You need to be able to know a protocol's applications, how it can be used to attack a network, and how to recognize if protocol transmission is out of the norm. You will sign up to write a study on a protocol of your choice and present your research to the class.

Security Product Audit and Presentation

The Product Evaluation Audit puts your protocol analysis and Autopsy analysis (including potential log analysis) to use in evaluating whether your two products adhere to your future organization's policies and whether the products extract and send information or modify the internals of a system.

Midterm and Final Exam

The midterm exam covers Wireshark protocol analysis and complete essay questions. The final exam requires you to analyze a case study and answer the questions posed.

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	94% - 100%
A-	90% - < 94%
B+	87% - < 90%
B	84% - < 87%
B-	80% - < 84%
C+	77% - < 80%
C	74% - < 77%
C-	70% - < 74%
F	0 - < 70%

Assignment	Percentage
Discussions	10%
Quizzes	10%
Labs and Exercises	10%
HWK 1: Protocol Presentation	15%
HWK 2: Security Product Audit Report	15%
HWK 2: Security Product Presentation	5%
Midterm	15%
Final Exam (Part 1 and Part 2)	20%
Total	**100%**