EEE4752 - Introduction to Network Forensics and Incident Response
Three Credits, Four and a half hours, Engineering Topic.

Instructor: Dr. Yu Du.

Textbook:

Specific Course Information:
This is undergraduate-level 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. Topics covered include forensics techniques, packet capture, log analysis, types of attacks, correlated attacks and network scanning and artifact acquisition.

Specific Goals for the Course
a. Specific outcomes of instruction
Upon successful completion of this course, the student will:
1. Evaluate the basics of network forensics.
2. Appraise the fundamental networking concepts and its protocols.
3. Analyze host-side artifacts.
4. Contrast the concepts related to packet capture and its processing for feature extraction.
5. Evaluate the different attack types associated with networking.
6. Illustrate the importance of location awareness of acquired information.
7. Contrast appropriate event logging and preparing for attacks.
8. Analyze the manner intrusion detection systems operate and what data they possess.
9. Analyze firewall and application logs for networking artifacts.
10. Evaluate the manner that attacks are correlated.
11. Appraise networking scanning techniques.
12. Correlate the information gathered through networking scanning.
13. Evaluate the implications of encryption on network forensics.
14. Analyze the cloud computing and its implication in determining artifacts.

b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.
In this course the student will have to show
(a) an ability to apply knowledge of mathematics, science, and engineering (N/A)
(b) an ability to design and conduct experiments (simulations), as well as to analyze, interpret data (N/A)
(c) an ability to design a system, component, or process to meet desired needs (N/A)
(d) an ability to function in multi-disciplinary teams (N/A)
(e) an ability to identify, formulate, and solve engineering problems (homework) (N/A)
(f) an understanding of professional and ethical responsibility (N/A)
(g) an ability to communicate effectively (through project reports) (N/A)
(h) the broad education necessary to understand the impact of engineering solutions in a global and societal context (N/A)
(i) a recognition of the need, and an ability to engage in life-long learning (N/A)
(j) a knowledge of contemporary issues (N/A)
(k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice (N/A)
(l) a knowledge of probability and statistics (N/A)

**Brief list of the topics to be covered**
1. Network Forensics and Incident Response Basics
2. Networking Fundamentals
3. Networking Fundamentals II
4. Search for Host-side Artifacts
5. Packet Capture and Analysis
6. Attack Types
7. Location Awareness
8. How to Prepare for an Attack
9. Intrusion Detection Systems
10. Using Firewall and Application Logs
11. Correlating Attacks
12. Network Scanning
13. Encryption and Cloud Computing

**GRADING:**

<table>
<thead>
<tr>
<th>Course Requirements</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes</td>
<td>15%</td>
</tr>
<tr>
<td>Exams</td>
<td>40%</td>
</tr>
<tr>
<td>Discussions</td>
<td>15%</td>
</tr>
<tr>
<td>Case Study</td>
<td>5%</td>
</tr>
<tr>
<td>Assignments</td>
<td>25%</td>
</tr>
<tr>
<td>Overall Grade</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Conversion of Numerical Grade to Letter Grad**

<table>
<thead>
<tr>
<th>Numerical Grade</th>
<th>Letter Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>95&lt;= A &lt;=100</td>
<td>A</td>
</tr>
<tr>
<td>90&lt;= A- &lt; 94</td>
<td>B+</td>
</tr>
<tr>
<td>87&lt;= B+ &lt; 89</td>
<td>B</td>
</tr>
<tr>
<td>83&lt;= B&lt; 86</td>
<td>B-</td>
</tr>
<tr>
<td>80&lt;= B-&lt; 82</td>
<td>C+</td>
</tr>
<tr>
<td>77 &lt;= C &lt; 79</td>
<td>C</td>
</tr>
<tr>
<td>70&lt;= C &lt; 76</td>
<td>C-</td>
</tr>
<tr>
<td>60 &lt;= D &lt; 69</td>
<td>D</td>
</tr>
<tr>
<td>F: Below 60</td>
<td>F</td>
</tr>
</tbody>
</table>