Instructor Information:
Deana Shick
dshick@cert.org
Office Hours: by appointment only

Kyle O’Meara
komeara@cert.org
Office Hours: by appointment only

TA Information:
Madison Oliver
mqo@andrew.cmu.edu
Office Hours: Monday 1830-1930 & by appointment

Email is the easiest and quickest form of communication for us. Please include both instructors on any correspondence and 95-855 in the email 'Subject' line. One of us will get back to you as soon as we can. There will be few delays in communication (we are human, too).

Bottom Line Up Front (BLUF):
• We will use Blackboard. Please check it often. You will submit your assignments there, too.
• Homework reading and assignments will be posted following class
• By the end of the course, you will be able to demonstrate network profiling and network analysis, analyze malicious behavior, and synthesize output from common network analysis tools.
• You will practice effective communication in the form of analysis summaries, and homework assignments.
• You are expected to effectively communicate with the instructors and others for both native and non-native English speakers.
• There will be a midterm, final, and small to medium sized projects/labs
• There will be ZERO cheating. We will punish any infraction to academic integrity to the full extent as outlined in our policies.

Course Management
Blackboard will be the used to post lecture notes, class materials, assignments, and other information. The onus is on the student to check Blackboard regularly for announcements, changes, and any other course information.

There will be several readings, videos, or other media provided to support the class lectures on Fridays. Students are expected to read/watch/interact with the course material to engage in
discussions on lecture days. The material provided in reading assignments will greatly help with leveling the learning curve for in class labs.

The instructors can make changes to the lecture schedule at any time in an effort to best serve the student and the overall needs of the class. A new syllabus will be provided to the students for any changes.

**Course Description**

This is a hands-on course that will survey network situational awareness techniques. The concept of network situational awareness is to develop a cogent set of observed network characteristics that will inform decision makers as to the wise course to take in defending the network (or more colloquially Know your network. Know the Internet. Know how they work together). The labs will involve network investigation to include packet capture analysis and network flow analysis.

**Micro:**
- What is the breadth of my network?
- What assets are important to my mission?
- What vulnerabilities affect me?
- How do I perform efficient network analysis? What does “the bad” look like?

**Macro:**
- What are the geo-political effects of various movements across the world?
- How do I provide an assessment of a global problem to decision makers?
- What are the downstream affects others face because of me?

**Business Impacts:**
- What will this security implementation have on my business?
- What do I do if my network is being used for malicious activity?
- Can I take advantage of new technologies?

**Objectives**

By the end of the course, students should perform the following:
- Demonstrate network analysis using Wireshark (tshark), tcpdump, Scapy, Snort, and/or SiLK to profile a network, and identify malicious behavior in support of the mission needs of an organization.
- Compare mission differences between Law Enforcement, Network Defense, and Intelligence for national security.
- Summarize security-community analysis and synthesize indicators of compromise (IOCs) in order to properly communicate to the C-suite, management, or other members of the security community.
- Begin creation of personal “brand” to use within the security community at large.
Grading Scale
A defined rubric will be provided to students before any projects. This class will follow the Heinz grading scale:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>98%</td>
</tr>
<tr>
<td>A</td>
<td>92%</td>
</tr>
<tr>
<td>A-</td>
<td>90%</td>
</tr>
<tr>
<td>B+</td>
<td>88%</td>
</tr>
<tr>
<td>B</td>
<td>82%</td>
</tr>
<tr>
<td>B-</td>
<td>80%</td>
</tr>
<tr>
<td>C+</td>
<td>78%</td>
</tr>
<tr>
<td>C</td>
<td>72%</td>
</tr>
<tr>
<td>C-</td>
<td>70%</td>
</tr>
</tbody>
</table>

Course Outline
Changes to the syllabus schedule will be sent by the instructors at least 1 week before the scheduled class time.

<table>
<thead>
<tr>
<th>Class</th>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8/31</td>
<td>Intro to Network Analysis, Situational Awareness, and Cyber Threats</td>
</tr>
<tr>
<td>2</td>
<td>9/7</td>
<td>Intro to Packet Analysis</td>
</tr>
<tr>
<td>3</td>
<td>9/14</td>
<td>Layer 2, Layer 3, Layer 4 and Services</td>
</tr>
<tr>
<td>4</td>
<td>9/21</td>
<td>Continue of Week 3</td>
</tr>
<tr>
<td>5</td>
<td>9/28</td>
<td>IDS/IPS</td>
</tr>
<tr>
<td>6</td>
<td>10/5</td>
<td>Intro to SiLK</td>
</tr>
<tr>
<td>7</td>
<td>10/12</td>
<td>Network Profiling with SiLK</td>
</tr>
<tr>
<td>8</td>
<td>10/19</td>
<td>Midterm</td>
</tr>
<tr>
<td>9</td>
<td>10/26</td>
<td>Guest Speaker</td>
</tr>
<tr>
<td>10</td>
<td>11/2</td>
<td>IoT Network Profiling &amp; Analysis</td>
</tr>
<tr>
<td>11</td>
<td>11/9</td>
<td>Structural Analysis</td>
</tr>
<tr>
<td>12</td>
<td>11/16</td>
<td>Data Fusion</td>
</tr>
<tr>
<td>13</td>
<td>11/23</td>
<td>Thanksgiving break (No Class)</td>
</tr>
<tr>
<td>14</td>
<td>11/30</td>
<td>Packet Manipulation with Scapy</td>
</tr>
<tr>
<td>15</td>
<td>12/7</td>
<td>Final Project</td>
</tr>
</tbody>
</table>
Class Breakdown

- There will be small to medium projects/labs/quizzes throughout the semester that will be completed in-class and outside of class time. The projects/labs/quizzes will total 30%.
- The midterm will cover lectures and reading assignments for the first half of class. The midterm will be 20% of your final grade.
- The final will be cumulative of the entire class. The final will be 40% of your entire grade.
- Participation during in class discussion, in class activities, or discussion board will be 10%.

Academic Integrity

Cheating and plagiarism will not be tolerated. Any infractions could result in a range of consequences, including failure of the course. We will be using cheating technologies (like Turnitin) when applicable to ensure zero violations to academic integrity.

- All student work is expected to be original. Citations are required for every piece of borrowed material in proper IEEE format. Examples of this format are available here: [http://www.ieee.org/documents/ieeecitationref.pdf](http://www.ieee.org/documents/ieeecitationref.pdf). In text citations must be provided after no more than three consecutive sentences.
- Students are expected to demonstrate their own thoughts and efforts within class projects or assignments. Along with exact copying of any words in a document, we will also be checking for exact sentence structure within a paragraph or synonym swaps.

Accommodations for Individuals with Disabilities

Please come speak to the instructors after the start of the first class so we can accommodate as appropriate.

Attendance

Your attendance and participation in class is critical to getting the most out of this class. Classes are designed to be interactive and often are most successful when they draw on challenges faced by students. We will be performing in class activities to evaluate students throughout the semester.

Extensions, Rescheduling Exams, Late Assignments, and Regrading

Extensions and rescheduled exams will only be provided in the dire circumstances. These will be evaluated on a case by case basis and will require documentation.

We will only consider regrading if notified within 24 hours in writing (email preferred) of receiving an assignment. The student should explain why they thought the grade is inaccurate within the email.

Students will be submitting all assignments through Blackboard. Any late assignments timestamped after the expected due date provided by the instructors will result in a zero. Extensions will be considered in a case by case basis if provided in writing to the instructors at least 24 hours prior to the submission date. If Blackboard is down, students must provide the assignment via email to both instructors.
Mobile Devices
There will be zero use of mobile devices during exams, quizzes, or other in class assignments.

Group Work
There will be group work in this class. Groups will be no larger than 5 students and will be chosen by the professors (we will not be doing a you-are-picked-last-in-dodgeball scenario).

Success in This Class
We understand that many of you are coming from different backgrounds and experiences. We appreciate this heterogeneous mixture, as it allows ideas to flow, and provides a great basis for in class discussion! You will be successful in this class if you take the time to understand the assigned readings, participate in class discussions and activities, identify when you are not understanding a topic, and communicate effectively with your peers and the instructors. The instructors are here to facilitate your learning, not impede it.

The security community is notorious for critiquing ideas. We 100% support this debate if substantiated with evidence. You will not be successful in this class if your critiques are made at the personal level. If you are, however, able to articulate yourself in projects, group work, exams and use evidence to support your claims, then you will be successful. We recognize that some students may be hesitant to speak in class, and we will provide other means to join into debates and discussions.

We want this to be a flexible class based on student interest and needs. We will be providing an assessment the first day of class to identify the skill set of the students. We will adjust the course according to the students’ proficiency level. Students will be successful if they remain flexible, and enjoy hands-on activities to promote learning objectives. You will be successful if you take the time to complete these activities either in a group or individually. Teaching one another different aspects of the class is invaluable to learning the material.