Carnegie Mellon
Heinz College

<table>
<tr><td><b>Course Information*</b></td><td>Course Title: 95-884 Network Defenses
Mini A1, Fall 2021
Instructors: Toby Meyer (tjmeyer@andrew.cmu.edu), Chris Rodman (crodman@andrew.cmu.edu)
Carnegie Mellon University
Pittsburgh, PA. 15213

Office Hours: By appointment only and via Zoom

Textbook: None. Readings may be posted on Canvas on a week-by-week basis.</td></tr>
<tr><td><b>Prerequisites (if applicable)</b></td><td>Students will be required have a basic understanding of networking concepts (TCP/IP, OSI Model, etc.) and know common Windows and Linux commands and functionality.

This is a graduate level course and students will be expected to put in the additional time and to research solutions on their own and learn any prerequisites skills that they do not currently possess.</td></tr>
<tr><td><b>Description</b></td><td>The course will take a hands-on approach to introduce students to the different network defenses that exists to block, mitigate, and detect cyber-attacks. Firewalls, intrusion detection systems (IDS), and network sniffers are just some of the tools that students will learn to deploy and configure in a live lab environment. Additionally, time will be spent learning how to analyze data to make conclusions about the network that is being monitored and actively attacked.</td></tr>
<tr><td><b>Course Materials (if applicable)</b></td><td>Documents posted on the course’s Canvas site and distributed in class.</td></tr>
<tr><td><b>Evaluation Method</b></td><td>The final grade will be out of 400pts (100%). The grading breakdown is listed below.

<table>
<tr><td>Externally Written or Canvas Assignments (1)</td><td>20pts (5%)</td></tr>
<tr><td>STEPfwd Graded Labs (10)</td><td>20pts each for a total of 200 (50%)</td></tr>
<tr><td>Quizzes (6)</td><td>10pts each for a total of 60 (15%)</td></tr>
<tr><td>Group Exercise Participation (1)</td><td>20 pts (5%)</td></tr>
<tr><td>Final Exam (1)</td><td>100pts (25%)</td></tr>
</table></td></tr>
<tr><td><b>Grading Scale</b></td><td>
<table>
<tr><td>A+   100%</td><td>B+ 87 - 89%</td><td>C+ 77 - 79%</td></tr>
<tr><td>A   93 - 99%</td><td>B   83 - 86%</td><td>C   73 - 76%</td></tr>
<tr><td>A-   90 - 92%</td><td>B- 80 - 82%</td><td>C-   70 - 72%</td></tr>
</table>

*A+ cannot be achieved by bonus points or curved grading</td></tr>
<tr><td><b>Grading Rubric/explanation of grades</b></td><td>Grading rubrics or scoring explanations will be developed to assess assignments. Rubrics will be made available to students before each assignment is due.

<b>Quizzes</b>:
A short quiz will be administered at the beginning of classes 2 through 7 consisting of multiple choice and fill-in-the-blank questions. These questions will be based on the previous class’ lecture.</td></tr>
</table>

Labs:
Labs will be modules within the STEPfwd environment that will focus on applying hands-on application to concepts learned in the lecture. Students will be required to complete each lab and will be tracked within the environment. Each lab will have progress or knowledge based assessments, whereas completion and correctness will determine the final score.

Labs may be available and may be completed earlier than the week assigned, but must be completed no later than the start of the class following their assignment by 04:39:59 PM.

Assignments:
Assignments will take different forms depending on the subject. Some will be done on personal computers and others may be submitted via Canvas. Each one will have explicit directions and guidance on the scoring which will be based on a mix of completion and correctly answered questions.

All assignments will be due before the start of the next week's class at 04:39:59 PM.

Late Policy:
Any assignment turned in late will face a 50% reduction for the first 24 hours that it is turned in late. After the 24 hours the assignment will receive a 0% grade. This policy will be STRICTLY enforced.

Final Exam:
The final exam will be a Canvas based examination that will draw on the knowledge and concepts learned in the lectures, labs, assignments, and group exercise. Questions may be specific to the content completed during the course, even content that was not previously graded. The final exam will be open book and notes.

Course/Topical Outline:

A weekly breakdown of topics and assignments (readings, assignments/labs, project due-dates)

Week 1 – (August 31st and September 2nd, 2021) **Instructor: Chris**	
Topic	• Defense Strategies • Overview of tools and technologies • Review of the OSI model and TCP/IP • STEPfwd Overview
Labs	• How to Conduct a Performance Based Assessment
Readings/Links	• OWASP Top Ten: https://owasp.org/www-project-top-ten/ • The OSI Model: https://en.wikipedia.org/wiki/OSI_model

Week 2 – (September 7th and 9th, 2021) **Instructor: Toby**	
Topic	• Network Analysis ○ Wireshark ○ TCPDump ○ NTop
Labs	• Packet Capture with Wireshark
Assignment	• Dissection of a PCAP file
Readings/Links	• Wireshark Download and Info: https://www.wireshark.org/

Week 3 – (September 14th and 16th, 2021) **Instructor: TBD**

Topic	• Firewalls and Network Segmentation ○ Endian ○ PfSense ○ Windows host firewalls
Labs	• PfSense vs Endian: Writing Effective Firewall Rules • IPv6 Configurations and Risks
Assignment	• None
Readings	• TBD

Week 4 – (September 21st and 22nd, 2021) **Instructor: TBD**	
Topic	• Intrusion Detection Systems ○ Snort ○ Bro ○ Security Onion
Labs	• A Comprehensive Suricata Test Drive • Analyzing IDS Alerts Using Snorby
Assignment	• None
Readings/Links	• https://www.sans.org/reading-room/whitepapers/intrusion/open-source-ids-high-performance-shootout-35772 • Security Onion: https://securityonion.net/

Week 5 – (September 28th and 30th, 2021) **Instructor: TBD**	
Topic	• Security Information and Event Management ○ Splunk ○ OS logging • ELK Stack
Labs	• Analyzing Log Events Using the Splunk Interface • Analyzing Suricata Network Alerts using the ELK Stack
Assignment	• None
Readings/Links	• ElasticStack: https://www.elastic.co/

Week 6 – (October 5th and 7th, 2021) **Instructor: TBD**	
Topic	• Network Flow Analytics ○ SiLK
Labs	• Using Standalone Bro to Analyze Network-based Attacks • Performing Flow Analysis with Argus and Silk.
Assignment	• None
Readings	• TBD

Week 7 – (October 12th and 14th, 2021)	
Topic	• Group Exercise (non-scored but participation is mandatory) • Student will work in small groups in a facilitated manner in order to analyze an incident that has occurred in a production network. • Activities will be identified and assessed via several quizzes for feedback on your findings

Week 8 – (Week of October 18th, exact date TBD)	
Topic	• Final Exam

Course Policies & Expectations

Attendance and Policies Surrounding COVID-19:
All students are expected to attend class in-person unless the instructors are notified ahead of time.

By exception, attendance for the hands-on sessions, held Thursdays during weeks 1-6, is optional. These sessions, however, are dedicated time for students to work through the labs with access to the TA and faculty. Support outside of this time is not guaranteed to be timely.

Students are required to attend and participate in the in-class exercise as a part of their final grade.

When students are unable to attend due to a COVID-19 diagnosis or are prevented from attendance due to quarantine, faculty will be notified and will find an arrangement to support the student’s continued progress in the course.

Course Capture
The lectures may be recorded to make them available on Canvas after class and/or for an individual student missing a class for medical reasons.

Students with Disabilities:
Our community values diversity and seeks to promote meaningful access to educational opportunities for all students. CMU and your instructors are committed to your success and to supporting Section 504 of the Rehabilitation Act of 1973 as amended and the Americans with Disabilities Act (1990). This means that in general no individual who is otherwise qualified shall be excluded from participation in, be denied benefits of, or be subjected to discrimination under any program or activity, solely by reason of having a disability.

If you believe that you need accommodations for a disability, please contact us ASAP, and we will work together to ensure that you have the correct access to resources on campus to assist you through your coursework and time at CMU.

Academic Integrity:
Carnegie Mellon University sets high standards for academic integrity. Those standards are supported and enforced by students, including those who serve as academic integrity hearing panel members and hearing officers. The presumptive sanction for a first offense is course failure, accompanied by the transcript notation “Violation of the Academic Integrity Policy.” The standard sanction for a first offense by graduate students is suspension or expulsion. Please see http://www.cmu.edu/academic-integrity/ for any questions.

The instructors of this course have a strong aversion to cheating of any kind and will hold no reservations enforcing CMU’s strict academic policy. Ethics and compliance are important in cybersecurity and must also be displayed in the classroom as well. This is especially recognized with the need to move to a more remote method of teaching and learning. Students should not collaborate on quizzes, assignments, labs, or exams with the expressed intent to cheat. You maydiscuss potential avenues for approaching the labs and their objectives, though the sharing of answers should not occur.

Cell Phones, Smartphones and other handheld wireless devices:
Other than during class breaks, please silence ring tones and refrain from engaging in calls, messaging or other use during class time. All devices must not be visible in any way during quizzes.

Policy Regarding Students Using English as a Foreign Language:
Assignments in this course are graded with reference to evidence of the acquisition of concepts, presentation format, and accuracy of information. Having done business in countries that use languages other than English, we understand that the use of an unfamiliar language can result in unusual word choices or grammatical errors that are not critical to the overall understanding of the information. Therefore, we will take into account your need to function in a language that may be unfamiliar to you. We will provide feedback as appropriate if we feel that language or grammar you have used in assignments would be best if it were configured in a different way.

Use of SU Canvas System for this course:
The Heinz School uses Carnegie Mellon University's Canvas system to facilitate distance learning as well as to enhance main campus courses. In this course, we will use the Canvas system generally to post lecture notes and related documents and to receive assignments electronically from students. To access Canvas go to www.cmu.edu/canvas

We welcome feedback during and after the course. Students are encouraged to share life-experiences in class. We are open to suggestions about class sequences, changes to the content and additional topics to cover.