Carnegie Mellon
Heinz College

<table>
<tr><td>Course Information*</td><td>Course Title: 95-884 Network Defenses
Mini Z5, Summer 2021
Instructors: Chris Herr, Toby Myer
Carnegie Mellon University
Pittsburgh, PA. 15213

Office Hours: TBD, may hold weekly Zoom office hours or by request

Textbook: None. Readings may be posted on Canvas on a week-by-week basis.</td></tr>
<tr><td>Prerequisites (if applicable)</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>Description</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>Course Materials (if applicable)</td><td>Documents posted on the course’s Canvas site and distributed in class.</td></tr>
<tr><td>Evaluation Method</td><td>The final grade will be out of 350pts (100%). The grading breakdown is listed below.

<table><tr><td>Externally Written or Canvas Assignments (1)</td><td>40pts (5%)</td></tr><tr><td>STEPfwd Graded Labs (9)</td><td>20pts each for a total of 160 (50%)</td></tr><tr><td>Quizzes (5)</td><td>10pts each for a total of 50 (15%)</td></tr><tr><td>Final Exam (1)</td><td>100pts (25%)</td></tr><tr><td></td><td>350 total points</td></tr></table></td></tr>
<tr><td>Grading Scale</td><td>A+ 100% B+ 87 - 89% C+ 77 - 79%
A 93 - 99% B 83 - 86% C 73 - 76%
A- 90 - 92% B- 80 - 82% C- 70 - 72%

*A+ cannot be achieved by bonus points or curved grading</td></tr>
<tr><td>Grading Rubric/explanation of grades</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.

Quizzes:
A short quiz will be administered at the beginning of weeks 1 through 5 consisting of multiple choice and fill-in-the-blank question types. These questions will be based on the week’s lecture and labs/assignments.</td></tr>
</table>

Labs:
Labs will be modules within the STEPfwd environment that will focus on applying hands-on concepts associated with the lecture topics. 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 completed earlier than the week assigned, but must be completed no later than the end the course week of their assignment by 11:59:59 PM on Sunday evenings.

Assignments:
Assignments will take different forms depending on the subject. Some activities will be done on personal computers and 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 end of the course week of their assignment by 11:59:59 PM on Sunday evenings.

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)

Introduction Materials	
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 (non-graded but will help you get familiar with the Lab Player interface)
Readings/Links	• OWASP Top Ten: https://owasp.org/www-project-top-ten/ • The OSI Model: https://en.wikipedia.org/wiki/OSI_model

Week 1 – (May 21-30, 2021)	

Topic	• Network Analysis
	  ○ Wireshark
	  ○ TCPDump
	  ○ NTop

Labs	• Traffic Analysis Using Wireshark (Analysis can also be done offline if desired via Canvas file download)
Assignment	• Dissection of a PCAP file
Readings/Links	• Wireshark Download and Info: https://www.wireshark.org/

Week 2 – (May 31 - June 6, 2021)	

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/Links	• TBD

Week 3 – (June 7-13, 2021)	

Topic	• Intrusion Detection Systems
	  ○ Snort
	  ○ Bro
	  ○ Security Onion

Labs	• Suricata – Installation, Configuration, and Defense • Analyzing IDS Alerts Using Security Onion
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 4 – (June 13-20, 2021)	

Topic	• Security Information and Event Management
	  ○ Splunk
	  ○ OS logging
	• ELK Stack

Labs	• Analyzing Web Server Log Events Using the Splunk Analyzing (Analysis can also be done offline if desired via Canvas file download) • Elastic Stack and Kibana – Default Dashboards
Assignment	• None
Readings/Links	• ElasticStack: https://www.elastic.co/

Week 5 – (June 20-26, 2021)	
Topic	• Network Flow Analytics ○ SiLK, Bro.
Labs	• Detecting an Unknown Attacker with Bro • Performing Flow Analysis with Argus and Silk.
Assignment	• None
Readings	• TBD

Week 6 – (June 27- July 3, 2021)	
Topic	• Final Exam *due by Saturday night due to holiday and grade deadlines

Course Policies & Expectations	**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 should be a part of every cyber security professional's character. **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.