Network Defenses
95844 A1 Spring 2024

Carnegie Mellon University

Instructor: Toby Meyer
Office hours: By Appointment
Phone: 412-268-6387
E-mail: tjmeyer@andrew.cmu.edu

Office hours: Refer to Course Site

Web site: ***http://www.cmu.edu/canvas/***

Course Management

All course materials will be managed through Canvas. Canvas will be used to post announcements of assignments and other information. Please be sure to check these announcements frequently to ensure you have the latest information about the course.

Textbook: None. Readings may be posted on Canvas on a week-by-week basis.

Prerequisites and Requirements

Students will be required to have a basic understanding of networking concepts (TCP/IP, OSIModel, 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 to research solutions on their own and learn any prerequisite skills they do not currently possess.

Course Description

The course takes a hands-on approach to introduce students to the different network defenses that exist 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.

Learning Objectives

Upon completion of this course, the student will obtain an understanding and will apply key concepts, including:

Learning Objective(s)
•Basic network fundamentals – including topologies, protocols, and services, and security issues affecting networks.

•Identify technical components supporting network defense
•Understand scenarios and use cases in which defense tactics may be applied
•Become familiar with network defense protocols, tools, and tactics required in modern computer networks
•Demonstrate how network defenses are applied according to policy requirements
•Foundational concepts of cyber and information security and the key practices and processes for managing security effectively.
•Key elements of incident management; detection, remediation, and recovery.
•Basic network fundamentals – including topologies, protocols, and services, and security issues affecting networks.
•Identify technical components supporting network defense
•Understand scenarios and use cases in which defense tactics may be applied
•Become familiar with network defense protocols, tools, and tactics required in modern computer networks

Each learning objective will be assessed via feedback during lectures, assignments, discussions, presentations, and examinations.

Schedule *(…subject to change during the semester)*

Introductory Material: January 16 – January 18, 2024
• Defense Strategies • Overview of tools and technologies • Review of the OSI model and TCP/IP • STEPfwd Overview
• How to Conduct a Performance Based Assessment
• OWASP Top Ten: https://owasp.org/www-project-top-ten/ • The OSI Model: https://en.wikipedia.org/wiki/OSI_model

Lesson 1: January 23 –January 25 2024	
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/

Lesson 2: January 30 – February 1, 2024

Topic	• Firewalls and Network Segmentation
	  o Endian
	  o PfSense
	  o Windows host firewalls

Labs	• PfSense vs Endian: Writing Effective Firewall Rules • IPv6 Configurations and Risks
Assignment	• None
Readings	• TBD

Lesson 3: February 6 – February 8, 2024	

Topic	• Intrusion Detection Systems
	  o Snort
	  o Bro
	  o 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/

Lesson 4: February 13 – February 15, 2024	

Topic	• Security Information and Event Management
	  o Splunk
	  o 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/

Lesson 5: February 20 – February 22, 2024	
Topic	• Network Flow Analytics o SiLK
Labs	• Using Standalone Bro to Analyze Network-based Attacks • Performing Flow Analysis with Argus and Silk.
Assignment	• None
Readings	• TBD

Final Exam: Week of February 26, 2024	
Topic	• Final Exam
Assignment	• Week 6 Quiz
Readings	• TBD

Evaluation Method

The final grade is out of 400pts (100%). The grading breakdown is as follows:

Externally Written or Canvas Assignments (1)	20pts (5%)
Foundry/Crucible Graded Labs (10)	20pts each for a total of 200 (50%)
Quizzes (6)	10pts each for a total of 60 (15%)
Presentation/In-class Participation (1)	20pts (5%)
Final Exam (1)	100pts (25%)

Grade Distribution

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

Grading Rubric/explanation of grades

Grading rubrics or scoring explanations will be developed to assess assignments. Rubrics will bemade available to students before each assignment is due.

Quizzes:
A short quiz will be administered at the beginning of classes 2 through 7 consisting of multiplechoice and fill-in-the-blank questions. These questions will be based on the previous class' lecture and labs/assignments.

Labs:
Labs will be modules within the Foundry/Crucible (alternatively 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 becompleted no later than the start of the class following their assignment.

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.

Research Presentation:
Students must gain skills and confidence in analyzing technical concepts and conveying them to others. Students in this course will develop a presentation based on publicly available sources that will demonstrate his/her ability to communicate technical constructs/challenges/issues clearly and effectively. Additional information regarding this assignment will be provided in Canvas.

Final Exam:

The final exam is delivered in Canvas and draws on the knowledge and concepts learned in the lectures, labs, assignments, and group project. 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.

Late assignment policy

Any **lab** turned in late will face a 50% reduction for the first 24 hours that it is turned in late. After 24 hours the assignment will receive a 0% grade. This policy will be STRICTLYenforced. I WILL NOT accept late **homework**, including **quizzes**, unless the student has made arrangements with me prior to the assignment's due date. *PRIOR ARRANGEMENTS MUST BE MADE NO LATER THAN 12 PM ON THE DUE DATE.*

Cheating and plagiarism

For all submissions for a grade, each student is responsible for handing in his/her own work. For any assignment found to be the partial or complete result of cheating or plagiarism, penalties will be enforced consistent with Carnegie Mellon University's Academic Disciplinary Actions. Cheating is defined as inappropriate collaboration among students on an assignment or exam or failure to cite the work of others. This can include copying someone else's work with or without alteration. When students are found to be collaborating in this way, *BOTH* will pay the penalty regardless of who originated the work. Please refer to the University Policies on Academic Integrity:
http://www.cmu.edu/policies/StudentPolicy.html https://www.cmu.edu/policies/student-and-student-life/academic-integrity.html https://www.cmu.edu/student-affairs/theword/academic-discipline/index.html

Use of Generative AI:

You may use generative AI programs like ChatGPT during the brainstorming and idea-generation phase for assignments, if applicable. However, doing so **cannot** be considered a **substitute** for traditional research. Generative AI programs rely on predictive models to generate content that may appear correct, but has been shown to sometimes be incomplete, inaccurate, taken without attribution from other sources, and/or biased. Any information generated by an AI program should be cited like any other reference material. You are ultimately responsible for the content of the information you submit. However, you may not attempt to pass off any work generated by an AI program as your own. Passing off any generated content as your own (for example - cutting and pasting content into written assignments, or paraphrasing AI content) constitutes an academic integrity violation. **If you have questions about using generative AI in this course, please talk to me.**

Take Care of Yourself

Do your best to maintain a healthy lifestyle this semester by eating well, exercising, avoiding drugs and alcohol, getting enough sleep, and taking some time to relax. This will help you achieve your goals and cope with stress.

All of us benefit from support during times of struggle. You are not alone. There are many helpful resources available on campus and an important part of the college experience is learning how to ask for help. Asking for support sooner than later is often helpful.

If you or anyone you know experience any academic stress, difficult life events, or feel anxiety or depression, we strongly encourage you to seek support. Counseling and Psychological Services (CaPS) is available to help: call 412.268.2922 and visit the website: http://www.cmu.edu/counseling/ . Consider reaching out to a friend, faculty or family member you trust for help getting connected to the support that can help.

Accommodations for Students with Disabilities:
If you have a disability and have an accommodations letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate. If you suspect that you may have a disability and would benefit from accommodations but are not yet registered with the Office of Disability Resources, I encourage you to contact them at access@andrew.cmu.edu.