CARNEGIE MELLON UNIVERSITY Heinz College

95-758 Network and Internet Security
Spring 2021, section A
Syllabus

General

Instructor/Course Support
Robert Beveridge: rbeverid@andrew.cmu.edu
Cell: (847) 238-2428

Office Hours and Location: By Appointment
Teaching Assistant: Hayden Moore: hmmoore@sei.cmu.edu

Please include both the instructor and the TA when emailing to get the fastest response.

Textbook
Corporate Computer Security, 5th Ed. (Boyle and Panko) ISBN-13: 978-0133545197
https://www.pearson.com/us/higher-education/program/Boyle-Pearson-e-Text-for-Corporate-Computer-Security-Access-Card-5th-Edition/PGM2616248.html

Course Description:

- Tuesdays 6:30PM - 9:20PM
- Location: HBH 1206 / Virtual
- 12 units

This course emphasizes practical employment of network security.
Topics in this course include:

- A working knowledge for the need to design networks
  - Properly support an organization
  - Properly accommodate networking protocols
  - Properly security an organization's cyber assets through its network infrastructure

Learning Objectives:

1. Application of security principles to computer networking
2. The OSI and TCP/IP models of network communications
3. Network security at different layers of the OSI and TCP/IP models
4. Enterprise systems for AAA
5. Security virtual machine and cloud-based IT infrastructure

6. Designing networks on selected protocols to support business operations while maintaining identified levels of network security
7. Supporting secondary network connectivity (wireless, VPNs, BYOD devices, partner networks, cross-domain and other connectivity types)
8. Designing networks to support Resiliency Management, Business Continuity, Disaster Recovery and other principles to avoid network failures that negatively impact the organizations ability to deliver on its core mission.
9. Methods to prevent, detect and respond to security breaches, including the role of incident response teams

Prerequisites
Required: successful completion of Introduction to Information Security Management (95-752) or equivalent experience in industry.
Additional: There is an expectation that students have a general knowledge of IT principles and cybersecurity topics

Course Management
All course materials will be managed through Canvas (www.cmu.edu/canvas). Canvas will be used to post announcements of assignments and other information. Check frequently to ensure you have the latest information about the course.
Topical readings that support the course lectures may be added. These readings will be posted under the course schedule portion of the syllabus. *Students are expected to read the material as part of the course materials.* In some cases, these readings will be integrated to homework assignments.

Course Updates and Changes
This syllabus represents the course plan as conceived at the beginning of the semester but is subject to change and modification by the instructor at any time. Advanced notice will be provided to students through Blackboard announcements, and when necessary, an updated syllabus will be issued.

External Resources and course videos
Cisco Networking Academy online courses
Cisco Networking Academy self-paced materials may be provided as a supplement for the course. The Academy courses will cover two different subjects: an introductory course in networking technologies for those who want to brush up on their networking skills, and a course in Cybersecurity Operations used for some assignments. See Extra Credit for more details.

Heinz STEPFWD
Self-paced experiential learning management system may be provided as part of the coursework.

Assignment Submissions
Assignments will be posted in Canvas. In emergency situations, you may also send them to the instructor AND to the TAs (please send to all in these cases).

Late Submissions Homework is due at 11:59 pm on the assigned due date (Pittsburgh local time). Penalty for late submissions is 2% per day (unless otherwise noted in the assignment). Assignments more than 5 days late will not be accepted. See the instructor (in advance if possible) to request exceptions.

Attendance Policy
As an online course, students are expected to manage their time to complete the course within the allotted course period.

Classroom Etiquette
This is a Master's level course taught as part of a professional degree program. Accordingly, you are expected to conduct yourself in a professional manner during the course, and not engage in behavior in the class that would be considered unacceptable in the workplace. This includes appropriate online etiquette in chat sessions or in correspondence with other students. If you have a question about the content of the lecture, please direct it to me or the Teaching Assistant. That way, you have a better chance of getting a prompt response. We will all use 'reply all' so that we all stay 'in the loop' on student correspondence.

Policy on Cheating and Plagiarism
For any assignment found to be the partial or complete result of cheating or plagiarism, your grade for that assignment will be zero. Cheating is defined as inappropriate collaboration among students on an assignment or failure to cite others' work used in the submissions, evaluation materials or presentations. This can include copying someone else's work with or without alteration. When students are found to be collaborating in this way, ALL COLLABORATORS will pay the penalty regardless of who originated the work. Please refer to the University's policies here: http://www.cmu.edu/policies/StudentPolicy.html

Grading Rubric Letter	Interpretation	Point Totals	GPA
A+	Exceptional	97 – 100	4.33
A	Excellent	93 – 97	4.00
A-	Very Good	90 – 93	3.67
B+	Good	87 – 90	3.33
B	Acceptable	83 – 87	3.00
B-	Fair	80 – 83	2.67
C+	Poor	75 – 80	2.33
C	Very Poor	70 – 75	2.00
D	Failing	Below 70	0

Proposed Schedule - Subject to Change

Week	Date	Topic	Assignments
1	Feb 2	Risk and OSI model	Wireshark Lab Cisco Intro Networking Pt1
2	Feb 9	Networking Protocols and Security	Cisco Intro Networking Pt2
3	Feb 16	Designing Network with IP and VLANS	Intro to Packet Tracer and Network Design
4	Feb 23	No Classes	
5	Mar 2	Secure Networks	Network Design
6	Mar 9	Access Controls	
7	Mar 16	Access Controls and Firewalls	Cisco - Snort and Firewall Rules Mid-Term Project
8	Mar 16	Windows Enterprise Security and Virtualization	Setup a multi-VM environment
9	Mar 23	Linux	Linux lab
10	Mar 30	Wireless security	Wireless Lab
11	Mar 30	Network Security Devices - IPS/IDS	IPS Lab
12	Apr 6	Remote access and VPN	VPN Lab
13	Apr 13	Data Management and resilience	
14	Apr 20	The NOC and SOC	
15	Apr 27	Final Project review	Final Project
16	May 4	Final Project Presentation	
17	May 11	Final Project presentation	