American Public University System

American Military University | American Public University

ISSC499

Course Summary

Course : ISSC499 **Title :** Senior Seminar in Cybersecurity
Length of Course : 8 **Faculty :**
Prerequisites : ENGL101, ENGL110 **Credit Hours :** 3

Description

Course Description:

This Capstone course is a senior level course designed to allow the student to review, analyze, and integrate the work the student has completed toward the Bachelors of Science in Cybersecurity degree. Students will examine a number of real-world scenario cases related to various aspects of Cybersecurity to complete various cybersecurity related plans and policies that demonstrate mastery of their program of study in a meaningful culmination of their learning and to assess their level of mastery of the stated outcomes of their degree requirements. (Prerequisite: Completion of a minimum of 105 hours towards your program including ENGL101 or ENGL110)

Course Scope:

This course presents students with an opportunity to investigate the various aspects of Cybersecurity including the relationship between cyber defense, cyber operations, cyber exploitations, cyber intelligence, cybercrime, Cyberlaw within Federal and State Laws. Students will be able to demonstrate an in-depth understanding of Cybersecurity as a discipline with many associations and complexities and to develop an understanding of how legal, ethical and criminal justice theories are applied.

This course blends together the vast issues and challenges associated with the discipline of Cybersecurity while emphasizing the need to conduct research associated with securing the United States cyberspace and safeguarding it from a myriad of threats both national and international. The overall goal is that each student will apply the knowledge and skills that have been obtained over the course of their undergraduate Cybersecurity studies to real-world challenges.

The capstone course is designed to polish students' writing, analytical, and research skills from the variety of discipline areas studied so that he or she may confidently confront the challenges and demands of specialized research and written communication. This course provides students with the opportunity to complete an approved academic research exercise or other creative scholarly activity resulting in a tangible product that demonstrates synthesis of a student's coursework and substantial knowledge of the Cybersecurity field of study. The course also addresses the notion of capstone by considering overall academic accomplishments in light of specific personal and career goals. This course is to be taken as the LAST course in the Cybersecurity program.

Objectives

The successful student will fulfill the following learning objectives:

CO-1: Examine the various aspects of cybersecurity including the relationship between cyber defense, cyber operations, cyber exploitations, cyber intelligence, cybercrime, Cyberlaw within Federal and State Laws

CO-2: Deconstruct the **processes and goals of cyber forensics investigations including the importance of search warrants and chain of custody in a forensic investigation of computer related crimes**

CO-3: Prepare a plan to manage functions that encompass overseeing a program or technical aspect of a security program at a high level ensuring currency with changing risk and threat environments.

CO-4: Prepare a plan to design functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.

CO-5: Develop strategies and plans for security architecture consisting of tools, techniques, and technologies to detect and prevent network penetration, and to design effective cybersecurity countermeasures.

CO-6: Develop a policy to analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management for wired, wireless, and satellite networks that affect the security of the cyberspace.

CO-7: Develop a policy to implement functions that encompass putting programs, processes, or policies into action within an organization.

CO-8: Prepare a plan to evaluate functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives.

Outline

Week 1: Begin the research process

Learning Objectives

CO-1: Examine the various aspects of cybersecurity including the relationship between cyber defense, cyber operations, cyber exploitations, cyber intelligence, cybercrime, Cyberlaw within Federal and State Laws.

Activities

Reading: Chapters 1

Reading: Supplemental Resources

Week 1 Introduction Discussion

Assignment #1

Week 2: Capstone Project development

Learning Objectives

CO-2: Deconstruct the processes and goals of cyber forensics investigations including the importance of search warrants and chain of custody in a forensic investigation of computer related crimes

Activities

Reading: Chapter 2

Reading: Supplemental Resources

Week 2 Discussion

Assignment #2

Capstone Project Topic selection (4 - 6 page idea paper)

Week 3: Cyber Doctrine

Learning Objectives

CO-3: Prepare a plan to manage functions that encompass overseeing a program or technical aspect of a security program at a high level ensuring currency with changing risk and threat environments.

Activities

Reading: Chapter 3

Reading: Supplemental Resources

Week 3 Discussion

Assignment #3

Week 4: Cyber Tools and Techniques

Learning Objectives

CO-4: Prepare a plan to design functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.

Activities

Reading: Chapter 4

Reading: Supplemental Resources

Week 4 Discussion

Assignment #4

Week 5: Offensive and Defensive Tactics and Procedures - Challenges We Face

Learning Objectives

CO-5: Develop strategies and plans for security architecture consisting of tools, techniques, and technologies to detect and prevent network penetration, and to design effective cybersecurity countermeasures.

Activities

Reading: Chapter 7

Reading: Supplemental Resources

Week 5 Discussion

Assignment #5

Week 6: Where is Cyber Warfare Headed

Learning Objectives

CO-6: Develop a policy to analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management for wired, wireless, and satellite networks that affect the security of the cyberspace.

Activities

Reading: Chapters 9

Reading: Supplemental Resources

Week 6 Discussion

Assignment #6

Week 7: Organization and argument in research

Learning Objectives

CO-7: Develop a policy to implement functions that encompass putting programs, processes, or policies into action within an organization.

Activities

Reading: Chapters 8

Reading: Supplemental Resources

Week 7 Discussion

Assignment #7

Week 8: Project completion

Learning Objectives

CO-8: Prepare a plan to evaluate functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives.

Activities

Reading: Chapter 6

Reading: Supplemental Resources

Week 8 Discussion

Assignment #8

Final Capstone Project (30 – 40 page Project paper)

Evaluation

Grading will be based on weekly assignments, discussions and a Capstone project.

1. There will be **weekly discussion** (2% each) counting a total of 16% of the final grade. Answers should restate the question with supporting sentences using the terms, concepts, and theories from the required readings. The key requirement is to express your idea and then support your position to demonstrate that you understand the material. Your answer should be substantive.

In addition, you are to **respond** to at least **two** of your classmates' postings by commenting on, supporting or supplementing the other students' answers. Your responses should be substantive. All responses should be courteous with sound supporting sentences. You may respond multiple times within a continuous discussion with points and counter points. Duplicate responses **will not** receive credit.

2. There will be eight assignments (totaling 40% of the course grade), which break down the process for the final capstone project. Each week you will be working on a portion of the Capstone project. **Assignments #1 – #8** each will cover the weekly course objective. These are 4-6 page papers using APA style formatting. In Week 8 you will be combining, summarizing, and culminating the final capstone project from the eight parts you have been working on through week 8. The Week 8 **Capstone Project** – (44%) will follow a conventional report format (introduction, body – comprising of the 8 parts discussed, conclusion, and references). The paper is to follow the APA style guide, Current Edition (available via bookstores). Also refer to APA's online resources: The Basics of Current Edition APA Style and the APUS web site: APUS Online Library.

Note: Review **Announcements** and **Lessons** for additional instructions and course materials.

3. All assignments and discussion responses are required by 11:59 PM Eastern Time of the Sunday of the week assigned.

Grading:

Name	Grade %
Assignments	40.00 %
Week # 1 Assignment	5.00 %
Week # 2 Assignment	5.00 %
Week # 3 Assignment	5.00 %
Week # 4 Assignment	5.00 %
Week # 5 Assignment	5.00 %
Week # 6 Assignment	5.00 %
Week # 7 Assignment	5.00 %
Week # 8 Assignment	5.00 %
Capstone Project	44.00 %
Capstone Project Topic Selection	7.33 %
Week # 8 - Final Capstone Project & Presentation	36.67 %
Discussions	16.00 %
Week 1: Introduction	2.00 %

Week 2: Cybersecurity Deductive Forensics	2.00 %
Week 3: Cybersecurity Objectives	2.00 %
Week 4: Defensive Programming	2.00 %
Week 5: Defensive Tactics and Procedures	2.00 %
Week 6: Cybersecurity Evolution	2.00 %
Week 7: Social Engineering Policy	2.00 %
Week 8: Cybersecurity Policy Effectiveness	2.00 %

Materials

Book Title: The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice - e-book available in the APUS Online Library

Author: Winterfeld, Steve

Publication Info: Syngress

ISBN: 9780124047372

Book Title: The 7 Qualities of Highly Secure Software - e-book available in the APUS Online Library

Author: Paul, Mano

Publication Info:

ISBN: 9781439814468

Book Title: Cybersecurity: Public Sector Threats and Responses - e-book available in the APUS Online Library

Author: Andreasson, Kim

Publication Info:

ISBN: 9781439846636

Book Title: Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives - e-book available in the APUS Online Library

Author: Raghu, Santanam

Publication Info: IGI Global

ISBN: 9781609601232

Book Title: To find the library e-book(s) req'd for your course, please visit to locate the eReserve by course #.

Author: No Author Specified

Publication Info:

ISBN: N/A

Required Text:

[The basics of cyber warfare [electronic resource] : understanding the fundamentals of cyber warfare in theory and practice / Steve Winterfeld, Jason Andress ; Andrew Hay, technical editor.](#) Winterfeld, Steve.; Waltham, Mass.; Syngress, ; c2013 ; [APUS Online Library](#).

[Cyber security, cyber crime and cyber forensics [electronic resource] : applications and perspectives / [edited by] Raghu Santanam, M. Sethumadhavan and Mohit Virendra.](#); Hershey, PA : ; Information Science Reference, ; c2011. ; "[This book provides broad coverage of technical and socio-economic perspectives for utilizing information and communication technologies and developing practical solutions in cyber security, cyber crime and cyber forensics](#)"--Provided by publisher. ;

From [Faulkners Security Management Database that APUS subscribes](#). This includes a link to a search page within the database - type in Cybersecurity to get a list of reports available.

Cybersecurity resources: link to a video: [U.S. Senate Committee on Commerce, Science & Transportation](#)

Cybersecurity: Cyber Crime Protection Security - link to the video for Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat: http://oversight.house.gov/hearing/cybersecurity-assessing-the-nations-ability-to-address-the-growing-cyber-threat/

Additional Supplemental Resources for Cybersecurity at the End of This Syllabus…

Software Requirements

1. Microsoft Office (MS Word, MS Excel, MS PowerPoint)
2. IE, Firefox, Google Chrome

Course Guidelines

Citation and Reference Style

- Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the APA Format.

Tutoring

- [Tutor.com](#) offers online homework help and learning resources by connecting students to certified tutors for one-on-one help. AMU and APU students are eligible for 10 free hours* of tutoring provided by APUS. Tutors are available 24/7 unless otherwise noted. Tutor.com also has a SkillCenter Resource Library offering educational resources, worksheets, videos, websites and career help. Accessing these resources does not count against tutoring hours and is also available 24/7. Please visit the APUS Library and search for 'Tutor' to create an account.

Late Assignments

- Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. The due date for each assignment is listed under each Assignment.
- Generally speaking, late work may result in a deduction up to 15% of the grade for each day late, not to exceed 5 days.
- As a working adult I know your time is limited and often out of your control. Faculty may be more flexible if they know ahead of time of any potential late assignments.

Turn It In

- Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. This is automatically processed through the Assignments area of the course.

Academic Dishonesty

- Academic Dishonesty incorporates more than plagiarism, which is using the work of others without citation. Academic dishonesty includes any use of content purchased or retrieved from web services such as CourseHero.com. Additionally, allowing your work to be placed on such web services is academic dishonesty, as it is enabling the dishonesty of others. The copy and pasting of content from any web page, without citation as a direct quote, is academic dishonesty. When in doubt, do not copy/paste, and always cite.

Submission Guidelines

- Some assignments may have very specific requirements for formatting (such as font, margins, etc) and submission file type (such as .docx, .pdf, etc) See the assignment instructions for details. In general, standard file types such as those associated with Microsoft Office are preferred, unless otherwise specified.

Disclaimer Statement

- Course content may vary from the outline to meet the needs of this particular group.

Communicating on the Discussion

- Discussions are the heart of the interaction in this course. The more engaged and lively the exchanges, the more interesting and fun the course will be. Only substantive comments will receive credit. Although there is a final posting time after which the instructor will grade comments, it is not sufficient to wait until the last day to contribute your comments/questions on the discussion. The purpose of the discussions is to actively participate in an on-going discussion about the assigned content.
- "Substantive" means comments that contribute something new and hopefully important to the discussion. Thus a message that simply says "I agree" is not substantive. A substantive comment contributes a new idea or perspective, a good follow-up question to a point made, offers a response to a question, provides an example or illustration of a key point, points out an inconsistency in an argument, etc.
- As a class, if we run into conflicting refer points, we must respect each individual's own opinion. Hateful and hurtful comments towards other individuals, students, groups, peoples, and/or societies will not be tolerated.

Identity Verification & Live Proctoring

- Faculty may require students to provide proof of identity when submitting assignments or completing assessments in this course. Verification may be in the form of a photograph and/or video of the student's face together with a valid photo ID, depending on the assignment format.
- Faculty may require live proctoring when completing assessments in this course. Proctoring may include identity verification and continuous monitoring of the student by webcam and microphone during testing.

University Policies

[Student Handbook](#)

- [Drop/Withdrawal policy](#)
- [Extension Requests](#)
- [Academic Probation](#)
- [Appeals](#)
- [Disability Accommodations](#)

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.