CSEC - 3758 - Offensive Cyber Operations

05. UG New Course No Special Designation

Due Dates and Resources

If you have questions or need assistance in filling out this proposal form, you may contact the Office of Curriculum.

Deadlines for curriculum can be found:

- Curriculum SharePoint
- Curriculum Website
- Procedural Calendar
- On your Curriculog dashboard under 'My Upcoming Events'

Resources for curriculum can be found:

- Originator How-To Guide
- Curriculum SharePoint

In order to meet the deadline, this proposal must be on the *Substantive College/School Level Review* step on or before the listed due date.

Directions for Form

General Instructions and Information

You may collapse individual sections of this form by clicking the arrow or "V" icon to the right of the section title.
All fields that are marked with an asterisk (*) are required.
Each section may have additional directions attached. Please follow all instructions.

Note: Proposals that are incomplete or filled out incorrectly will be returned to the originator.

INSTRUCTIONS FOR CREATING A NEW COURSE

Fill out all of the below fields.
Launch the proposal.
Approve the proposal.

Use the checkmark icon on the right of the screen to approve the proposal.

This form **SHOULD** be used only for the following:

- Creating a new course without a special designation (General Studies, Service Learning, Ethnic Studies & Social Justice, or Senior Experience).

This form **SHOULD NOT** be used for the following:

- Creating a new course with a special designation (General Studies, Service Learning, Ethnic Studies & Social Justice, or Senior Experience).
- Converting an omnibus or individual variable topic course into a regular course. Please use form #4 to complete this request.
- Making modifications to any course
- Creating or modifying graduate courses.

Part I: Department and Originator Information

College/School:* College of Aerospace, Computing, Engineering, and Design

Department:* Department of Computer Sciences

Name of Proposal Originator:* Klaus Streicher

Email of Proposal Originator:* Nstreich@msudenver.edu

Part II: Curriculum Proposal Justification and Resource Implication

Justification and resource implication for proposed curriculum action:*

CSEC 3758 Offensive Cyber Operations:

Offensive cyber operations are carefully planned operations that are executed in and through cyberspace to achieve actions on objectives. This course serves a the final (non senior experience) course in the CSCP course sequence and will reflect a culmincation of student coursework and experience up until this point.

This course will serve as a core course and supports NSA CAE-CO & ABET learning outcomes for the proposed Computer Security degree.

Related Curriculum Proposals:* https://msudenver.curriculog.com/proposal:11729/form

According to the Undergraduate Curriculum Manual, it is the responsibility of both the originator as well as each level of review to consider potential overlap and curriculum conflict. Any potential overlap or conflict with existing curriculum should be reviewed, and the impacted department(s) should be requested to provide a letter of notification or support, depending on the circumstances.

Attach documentation that supports affected Departments were notified and/or provided support of the proposed changes in the Proposal Toolbox by clicking on the paperclip icon on the right side of the form.

Please Confirm That:* ☑ I, the originator of this proposal, have completed the necessary due diligence to review this proposal for any potential overlap and/or conflict with existing curriculum. Any departments identified as having potential overlap and/or conflicts have been contacted and a letter of notification and/or a letter of support has been obtained.

Part III: Course Information

Is the identified course prefix a new course prefix? *
- ☑ Yes
- ☐ No

Prefix:* CSEC

Course Number:* 3758

CSEC

Course Title:* Offensive Cyber Operations

Transcript/Banner Course Title:* Offensive Cyber Operations

Course Type:* Computer Security

CIP Code: 11.1003

Please check all that apply from the selections below. You may select more than one option if applicable.

Check All that Apply:*
- [x] Required for Major
- [ ] Required for Minor
- [ ] Required for Concentration
- [ ] Required for Certificate
- [x] Elective
- [ ] Specified Elective

To receive Title IV financial aid funds, all institutions of higher education must comply with the federal definition of a credit hour. The Higher Learning Commission requires institutions to maintain policies and procedures for verifying compliance with this definition.

Federal Credit Hour Definition: *A credit hour is an amount of work represented in intended learning outcomes and verified by evidence of student achievement that is an institutionally-established equivalency that reasonably approximates not less than:*
(1) one hour of classroom or direct faculty instruction and a minimum of two hours of out-of- class student work each week for approximately fifteen weeks for one semester or trimester hour of credit, or ten to twelve weeks for one quarter hour of credit, or the equivalent amount of work over a different amount of time; or (2) at least an equivalent amount of work as required in paragraph (1) of this definition for other activities as established by an institution, including laboratory work, internships, practica, studio work, and other academic work leading toward to the award of credit hours. 34CFR 600.2 (11/1/2010)

Credits:* 4

Distribution of Credits:* 4 + 0

Schedule Type(s):* Lecture

Grade Mode(s):* Letter

Face-to-Face or Equivalent Hours per course

Consult Appendix B and C of the Curriculum Manual to determine the hours for the course

Lecture: 50

Lab:

Internship:

Practicum:

Other Hours:

Additional Student Work Hours: 120

Please answer yes or no to the below questions. If you answer yes to any of the questions, please fill out the related field on the right.

A specified repeatable course is a course that allows a student to repeat the course either in its entirety or for a certain identified total number of credit hours. If you decide to make your course repeatable, please specify either how many times a student can repeat the course for credit, or for the total number of credits they can receive.

Is this course a specified repeatable course?* (•) No ( ) Yes

If yes, indicate specified repeatable number of credits and/or repeats allowed:

Is this course a variable topics umbrella course?* (•) No ( ) Yes

If yes, indicate variable topic number of credits and/or repeats available:

A crosslisting is when a course is made available under additional prefixes for students in other programs.

An equivalency is when two courses are coded in Banner to be equal to each other.

Generally equivalencies are used when an old, archived course is needed to be equal to a new course. Crosslistings are used for all active courses. Supporting documentation should be included to demonstrate approval for crosslistings.

Are there course equivalencies?* (•) No ( ) Yes

If yes, list all equivalent courses in alphabetical order:

Will this course be requesting a crosslisting with any other prefix(es)?* (•) No ( ) Yes

If yes, list all crosslistings in alphabetical order:

Registration Restrictions

Program:

Major:

Level: Undergraduate

Class:

Student Attribute:

The following fields will allow you to attach prerequisites, corequisites, or prerequisites or corequisites to your course. Please specify if you want and of these prerequisites, corequisites, or prerequisites or corequisites Banner enforced.

Banner enforcement means that the requirement will be enforced when the student attempts to register for a course. If you do not Banner enforce the requirement, the system will not check the student's record for the requirement to be met.

Please also indicate the minimum passing grade.

Prerequisite(s):	CSEC 3755 AND CSEC 3756
Banner Enforced Prerequisite(s):	CSEC 3755 AND CSEC 3756
Minimum Passing Grade for Banner Enforced Prerequisite(s):	C- or T
Corequisite(s):	
Banner Enforced Corequisite(s):	
Prerequisite(s) or Corequisite(s):	
Banner Enforced Prerequisite(s) or Corequisite(s):	
Minimum Passing Grade for Banner Enforced Prerequisite(s) or Corequisite(s):	

Part III: Course Information, continued

Catalog Course Description:*	Students engage with advanced techniques in offensive cyber operations. Through a combination of theoretical frameworks and hands-on labs, they develop the skills necessary to conduct comprehensive cyber operations in a controlled environment. Emphasis is placed on performing sophisticated cyber tasks, such as gathering intelligence, identifying vulnerabilities, and executing complex cyber attacks. Students navigate and manipulate systems using a variety of tools and techniques, while also gaining experience in evasion and covert communication. Throughout the course, students practice applying these skills in practical scenarios, achieving specific objectives while operating under constraints

The note field DOES show up in the course listing in the university catalog. A note should be made in specific instances where additional information about a course needs to be conveyed to students. The most common reasons for adding a note are:

The course is crosslisted Example: *(Note: Credit will be granted for only one prefix.)*
Variable credit courses Example: *(Note: Variable Credit)*
A course is repeatable Example: *(Note: This course may be repeated up to 3 times under different topics)* OR *(Note: This course is repeatable for a maximum of six semester hours)*
If a student cannot take two courses and earn credit for both Example: *(Note: Students cannot earn credit for XXX1234 and XXX2345)*

Note:

Lab Fees: **Field Trips:**

Part III: Course Information, continued

The following section is the course content. You must adhere to the following format for each section:

Required reading: Please list materials in preferred citation style (eg. MLA, APA, etc.).

List each material in this format. If there are multiple materials please format them in a bullet or list style

Specific Measurable Student Behavioral Learning Objectives: Please list the SBLOs in your preferred numbering or bulleting style. Start section with: Upon completion of this course, the student should be able to:.
Detailed Outline of Course Content or Outline of Field Experience/Internship: Please list the course outline in your preferred numbering or bulleting style. It is recommended that you use a numbering format for this field.
Evaluation of Student Performance: Please list the evaluation of student performance in your preferred numbering or bulleting style.

You must use the numbering list feature within the toolbar above each field. Right click on a number in the list and select "Numbered List Properties" to change the numbering style. Please maintain consistency in the selected numbering or bulleting styles.

Required reading and other materials will be equivalent to:*

DeSousa, P. (2018). *The Hacker Playbook 3: Practical Guide to Penetration Testing*. CreateSpace Independent Publishing Platform.

Georgia Weidman. 2014. *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, San Francisco, CA, 528 pages. ISBN: 978-1-59327-564-8.

Eugene Lim. 2025. *From Day Zero to Zero Day*. No Starch Press, San Francisco, CA, 304 pages. ISBN: 978-1-7185-0394-6.

Specific, Measurable Student Behavioral Learning Objectives:*

Upon completion of this course, students should be able to

1. Perform open-source intelligence on organizations and individuals.

2. Conduct enumeration and scanning of target networks.

3. Conduct various types of cyber attacks using tools, custom software, and scripts.

4. Identify vulnerabilities in target organizations, systems, and networks.

5. Write malware to exploit vulnerabilities.

6. Gain unauthorized access to computer systems.

7. Define and achieve actions on objectives in target systems.

8. Employ techniques for evading detection including covert communications.

Detailed Outline of Course Content (Major Topics and Subtopics) or Outline of Field Experience/Internship *

1. Mission Planning and Execution

- Defining Mission Objectives and Goals
- Rules of Engagement (ROE) and Legal Considerations
- Target Selection and Prioritization
- Resource Allocation and Team Roles
- Operational Risk Management and Contingency Planning
- Timeline Development and Execution Phases
- Post-Operation Review and Reporting

2. Cyber Attack Frameworks

- Overview of Cyber Attack Frameworks (e.g., MITRE ATT&CK, Cyber Kill Chain)
- Mapping Attack Vectors to Framework Stages
- Tactics, Techniques, and Procedures (TTPs)
- Leveraging Frameworks for Adversary Emulation

3. Open-Source Intelligence (OSINT)

- OSINT Collection Techniques and Tools
- Analyzing Publicly Available Information (e.g., social media, databases)
- Identifying Critical Assets and Exposed Data
- Building Target Profiles
- Integrating OSINT into Offensive Cyber Operations
- Counter-OSINT and Deception Techniques

4. Cyber Attack Tools

- Overview of Common Attack Tools (e.g., Metasploit, Cobalt Strike, Nmap)
- Tool Selection Criteria Based on Operation Goals
- Custom Tool Development and Scripting (e.g., Python, PowerShell)
- Managing and Operating Attack Infrastructure
- Bypassing Security Measures with Advanced Tools

5. Privilege Escalation

- Understanding Privilege Levels and Access Controls
- Exploiting Local and Remote Vulnerabilities
- Credential Harvesting and Reuse
- Leveraging Misconfigurations and Weaknesses
- Post-Exploitation Strategies and Maintaining Persistence

6. Shellcode

- Shellcode Fundamentals (What is Shellcode?)
- Writing and Customizing Shellcode (x86/x64)
- Shellcode Injection Techniques
- Evasion Techniques for Antivirus and Endpoint Detection and Response (EDR)

- Shellcode in Exploit Development

7. Packet Crafting

- Fundamentals of Network Protocols and Packet Structure
- Tools for Packet Crafting (e.g., Scapy, Hping, Netcat)
- Creating and Manipulating Packets for Exploitation
- Techniques for Network Scanning, Spoofing, and Sniffing
- Detecting and Mitigating Crafted Packet Attacks

8. Command and Control (C2)

- C2 Infrastructure Setup and Management
- Communication Channels (e.g., HTTP, HTTPS, DNS, Custom Protocols)
- Stealth Techniques for C2 Communication
- Using and Modifying C2 Frameworks (e.g., Cobalt Strike, Empire)
- Detecting and Disrupting C2 Channels

9. Data Exfiltration

- Identifying and Classifying Sensitive Data
- Techniques for Extracting Data (e.g., File Transfer, Compression, Encryption)
- Covert Data Exfiltration Methods (e.g., DNS Tunneling, Steganography)
- Detection and Prevention Measures for Data Exfiltration
- Real-World Examples of Data Exfiltration

10. Actions on Objectives

- Defining Objectives After Initial Compromise
- Lateral Movement Techniques
- Gaining Long-Term Access and Persistence
- Data Manipulation and Destruction Tactics
- Endgame Strategies: Disruption, Degradation, Denial, Deception

11. Techniques for Evading Detection

- Bypassing Antivirus and Endpoint Detection (EDR/XDR)
- Utilizing Obfuscation and Encryption for Payloads
- Leveraging Legitimate Tools (Living off the Land - LOLBins)
- Detecting and Defeating Network Security Measures (e.g., IDS/IPS)
- Anti-Forensics Techniques

12. Covert Communication and Steganography

- Principles of Covert Communication
- Techniques for Concealing Communication (e.g., Steganography, Covert Channels)
- Utilizing Digital Media for Hidden Messages
- Detection and Analysis of Steganographic Techniques
- Countermeasures and Mitigation for Covert Communication

Evaluation of Student Performance:* Student evaluations can include asessments of the following types:

1. Homework assignments
2. Projects
3. Quizzes and/or exams
4. Active participation

CAEPD and Registrar's Office Use Only

Notes Director corrected a wrong course number in the Banner prerequisite field after confirming with the originator it was inaccurate.

This course modification will be effective for the University 2025-2026 Undergraduate Catalog via the Summer 2025 Catalog Addendum and will be available in Banner beginning in Spring 2026.

Form Revised July 2024