CS - 3755 - Computer Security Offense and Defense

05. UG New Course No Special Designation

Due Dates

Deadlines for curriculum can be found:

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

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

Please read instructions and information below before you begin your curriculum proposal. You may also consult the following resources which can provide additional assistance in understanding this form and the curriculum process.

- **Originator How-To Guide**
- **Curriculum SharePoint**
- **Example Proposal**

This form SHOULD be used for the following:

- **Creating a new course without a special designation (General Studies, Service Learning, Multicultural, or Senior Experience).**

This form SHOULD NOT be used for the following:

- **Creating a new course with a special designation (General Studies, Service Learning, Multicultural, or Senior Experience).**
- **Converting an omnibus or individual variable topic course into a regular course. Please use form #8 to complete this request.**
- **Making modifications to any course**
- **Creating or modifying graduate courses.**

Instructions:

Fill in all fields below

Launch the Proposal

Approve the proposal

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

Additional 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 instructions. Proposals that are incomplete or filled out incorrectly will be returned to the originator.

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

Department and Originator Information

College/School:* College of Health and Applied Sciences

Department:* Department of Computer Sciences

Name of Proposal Originator:* Steve Beaty

Email of Proposal Originator:* beatys@msudenver.edu

Curriculum Proposal Justification and Resource Implication

Justification and Rationale for Curriculum Proposal:* This is a new CS upper-division elective to help address the growing concerns over cybersecurity.

Resource Implication Narrative:* There are no additional resources needed as the course will be taught in-load.

Related Curriculum Proposals:* N/A.

Course Title Information

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

Prefix:* CS

Course Number:* 3755

Course Title:* Computer Security Offense and Defense

Transcript/Banner Course Title:* Comp Sec Off and Def

Course Type:* Computer Science

CIP Code: 11.0701

Course Hours, Restrictions, and Repeat Information

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

Check All that Apply:*
- ☐ Required for Major
- ☐ Required for Minor
- ☐ Required for Concentration
- ☐ Required for Certificate
- ☑ 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:	60	**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.

Is this course a specified repeatable course?*	◉ No ○ Yes	**If yes, indicate specified repeatable number of credits and/or repeats allowed:**	

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 variable topics umbrella course?*	◉ No ○ Yes	**If yes, indicate variable topic number of credits and/or repeats available:**	
Are there course equivalencies?*	◉ No ○ Yes	**If yes, list all equivalent courses:**	

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.

Will this course be requesting a crosslisting with any other prefix(es)?*	◉ No ○ Yes	**If yes, list all crosslistings:**	

Registration Restrictions

Program:		**Major:**	
Level:		**Class:**	
Student Attribute:			

Student Attributes:

Catalog Course Information

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. If you do not indicate a minimum passing grade, it will default to a "D-" and you will be required to complete another curriculum proposal to modify this minimum passing grade, even if your program has a different minimum passing grade.

Prerequisite(s):	CS3700 with "C-" or better, or permission of instructor
Banner Enforced Prerequisite(s):	CS3700
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):	
Catalog Course Description:*	This course covers the basics of performing vulnerability assessments for networks, computers, and programs. Coverage includes reconnaissance and exploitation tools, injections, weak passwords and authentication, and memory corruption techniques. The course also covers defense techniques including firewalls, intrusion detection/prevention systems, log analysis, event correlation, and security information and event management. The course addresses how programs are compromised via buffer overflows and heap corruption, along with techniques to counter those attacks.

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:**

Course Content

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

Required reading: Smith, J.R. (2014). ***Book of Examples*****. New York, NY: McGraw-Hill**

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: 1, a, i, ii, etc.
Detailed Outline of Course Content or Outline of Field Experience/Internship: I, A, 1, a, etc.
Evaluation of Student Performance: 1, a, i, ii, etc.

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 to adhere to the above formatting requirements.

Required reading and other materials will be equivalent to:*

- Kim, Peter (2018), *The Hacker Playbook 3: Practical Guide To Penetration Testing,* Independently published

AND

- Erickson, Jon (2008), *Hacking: The Art of Exploitation, 2nd Edition*, No Starch Press

Specific, Measurable Student Behavioral Learning Objectives:*

Upon completion of this course, the student should be able to:

1. Formulate approaches to performing reconnaissance.
2. Analyze the results from network scans.
3. Appraise the results of audits for servers and services.
4. Compose a toolkit for penetration testing.
5. Given a particular platform and network architecture, create a plan for testing its weaknesses.
6. Evaluate several approaches to intrusion detection and prevention.
7. Design a stateful packet filtering firewall.
8. Analyze log files using appropriate tools.
9. Assess the various techniques for creating and deploying malware.
10. Construct effective programming defenses against typical attacks.

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

I. Introduction to computer security
  A. Confidentiality, Integrity, Availability
II. TCP/IP Security
  A. Transport Layer Security
  B. IP Security
III. Web application vulnerabilities
  A. Injections
  B. Cross-site scripting
IV. Operating System and application exploitation
  A. Buffer and stack overflows
  B. Heap corruption
  C. Countermeasures
    1. Address Space Layout Randomization
    2. Canaries
V. Tools for vulnerability assessment
  A. Network scanners
  B. Host auditing
  C. Passwording
    1. Cracking and countermeasures
VI. Defending networks
  A. Network intrusion detection systems
  B. Firewalls
  C. Virtual Local Area Networks
  D. Virtual Private Networks
VII. Defending Hosts
  A. Host intrusion detection systems
  B. Anti-virus and -malware
VII. Introduction to malware analysis
  A. Types of malware and infection vectors
  B. Exploiting kernel calls
IX. Protecting users
  A. Training needs
  B. Anti-phishing
X. Ethics
XI. Regulations

Evaluation of Student Performance:* A combination of the two or more of the following.

1. Tests/Exams.
2. Security Experiments and Analysis.
3. Assignments.

Review for Conflict and Overlap

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. Full information on overlap/conflict can be found here.

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.

Academic Affairs and Registrar's Office Use Only

Notes

The link above: https://www.msudenver.edu/curriculum/formsandresources/ no longer works. I believe the new link should be: https://www.msudenver.edu/curriculum/manual/

Confirmed that course number is available for use.

This new course will be effective with the Summer 2022 catalog addendum for the University 2022-2023 Undergraduate Catalog and will be reflected in Banner beginning in Spring 2023.

Form Revised May 2021

Signatures for CS - 3755 - Computer Security Offense and Defense

There are no signatures required on this proposal.