Chair: Tracy Christofero | **GC#6: Course Addition**

Request for Graduate Course Addition

1. Prepare one paper copy with all signatures and supporting material and forward to the Graduate Council Chair.
2. E-mail one identical PDF copy to the Graduate Council Chair. If attachments included, please merge into a single file.
3. ***The Graduate Council cannot process this application until it has received both the PDF copy and the signed hard copy.***

College: CITE Dept/Division: Computer Science Alpha Designator/Number: CYBR/615 (•) Graded ( ) CR/NC

Contact Person: Dr. Wook-Sung Yoo Phone: x5452

NEW COURSE DATA:

New Course Title: Cybersecurity Vulnerability Assessment

Alpha Designator/Number: C Y B R / 6 1 5

Title Abbreviation: C y b e r V u l n e r a b i l i t y A S S E .

(Limit of 25 characters and spaces)

Course Catalog Description: (Limit of 30 words)

This course focuses on the complete cycle of enterprise security from identifying vulnerabilities, detecting application exploitation and post exploitation mitigations and analysis for an enterprise level cyber infrastructure.

Co-requisite(s): None First Term to be Offered: Fall 2019

Prerequisite(s): None Credit Hours: 3

Course(s) being deleted in place of this addition (*must submit course deletion form*): NA

Signatures: if disapproved at any level, do not sign. Return to previous signer with recommendation attached.

Dept. Chair/Division Head Yoo, Wook-Sung	Date 9/17/18
Registrar 110101	Date 9/21/18
College Curriculum Chair	Date 9/26/18
Graduate Council Chair	Date

Request for Graduate Course Addition - Page 2

College: CITE | Department/Division: Computer Science | Alpha Designator/Number: CYBR/615

Provide complete information regarding the new course addition for each topic listed below. Before routing this form, a complete syllabus also must be attached addressing the items listed on the first page of this form.

1. FACULTY: Identify by name the faculty in your department/division who may teach this course.

Paulus Wahjudi, Ph.D.
Cong Pu, Ph.D.

2. DUPLICATION: If a question of possible duplication occurs, attach a copy of the correspondence sent to the appropriate department(s) describing the proposal. Enter "***Not Applicable***" if not applicable.

Not Applicable

3. REQUIRED COURSE: If this course will be required by another deparment(s), identify it/them by name. Enter "***Not Applicable***" if not applicable.

Not Applicable

4. AGREEMENTS: If there are any agreements required to provide clinical experiences, attach the details and the signed agreement. Enter "***Not Applicable***" if not applicable.

Not Applicable

5. ADDITIONAL RESOURCE REQUIREMENTS: If your department requires additional faculty, equipment, or specialized materials to teach this course, attach an estimate of the time and money required to secure these items. (Note: Approval of this form does not imply approval for additional resources.) Enter "***Not Applicable***" if not applicable.

Not Applicable

6. COURSE OBJECTIVES: (May be submitted as a separate document)

Please see attached document

7. COURSE OUTLINE (May be submitted as a separate document)

Please see attached document

8. SAMPLE TEXT(S) WITH AUTHOR(S) AND PUBLICATION DATES (May be submitted as a separate document)

Please see attached document

9. EXAMPLE OF INSTRUCTIONAL METHODS (Lecture, lab, internship)

Please see attached document

10. EXAMPLE EVALUATION METHODS (CHAPTER, MIDTERM, FINAL, PROJECTS, ETC.)

Exam, Homework Assignments and Projects

11. ADDITIONAL GRADUATE REQUIREMENTS IF LISTED AS AN UNDERGRADUATE/GRADUATE COURSE

Not applicable

12. PROVIDE COMPLETE BIBLIOGRAPHY (May be submitted as a separate document)

Please see attached document

Request for Graduate Course Addition - Page 5

Please insert in the text box below your course summary information for the Graduate Council agenda. Please enter the information exactly in this way (including headings):

Department:
Course Number and Title:
Catalog Description:
Prerequisites:
First Term Offered:
Credit Hours:

Department: Computer Science
Course Number and Title: CYBR 615 Cybersecurity Vulnerability Assessment
Catalog Description: This course focuses on the complete cycle of enterprise security from identifying vulnerabilities, detecting application exploitation and post exploitation mitigations and analysis for an enterprise-level cyber infrastructure.
Prerequisites: None
First Term Offered: Fall 2019
Credit Hours: 3

BIBLIOGRAPHY

Advanced Penetration Testing: Hacking the World's Most Secure Networks by Will Allsopp, ISBN-13: 978-1119367680 , ISBN-10: 1119367689

Penetration Testing Essentials 1st Edition by Sean-Philip Oriyano, ISBN-13: 978-1119235309 ISBN-10: 1119235308

Alfred Menezes, Paul van Oorschot, Scott Vanstone, Handbook of Applied Cryptography, CRC Press; 1 edition (October 16, 1996), ISBN-10: 0849385237/ISBN-13: 978-0849385230

The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition, Dafydd Stuttard ISBN-13: 978-1118026472 ISBN-10: 1118026470

CYBR 615 Cybersecurity Vulnerability Assessment

Course Title/Number	Cybersecurity Vulnerability Assessment /CYBR 615
Semester/Year	Fall/2019
Days/Time	TBD
Location	TBD
Instructor	TBD
Office	TBD
Phone	TBD
E-Mail	TBD
Office Hours	TBD
University Policies	By enrolling in this course, you agree to the University Policies listed below. Please read the full text of each policy by going to www.marshall.edu/academic-affairs and clicking on "Marshall University Policies." Or, you can access the policies directly by going to www.marshall.edu/academic-affairs/policies/. Academic Dishonesty/Excused Absence Policy for Undergraduates/Computing Services Acceptable Use/Inclement Weather/Dead Week/Students with Disabilities/Academic Forgiveness/Academic Probation and Suspension/Academic Rights and Responsibilities of Students/Affirmative Action/Sexual Harassment

Course Description

This course focuses on the complete cycle of enterprise security from identifying vulnerabilities, detecting application exploitation and post exploitation mitigations and analysis for an enterprise-level cyber infrastructure.

Course Student Learning Outcomes

Course Student Learning Outcomes	How students will practice each outcome in this Course	How student achievement of each outcome will be assessed in this Course
Students will be able to perform risk assessment	Homework assignments, In class examples, Group discussions	Graded exam problems Graded homework assignments
Students will be able to various security testing and analysis tools	Homework Assignments, In class examples Group discussions	Graded exam problems Graded homework assignments
Students will be able to analyze common security loopholes and identify the cause	Homework, In class examples	Graded exam problems Graded homework assignments

CYBR 615 Cybersecurity Vulnerability Assessment Course Syllabus

Required Texts, Additional Reading, and Other Materials

Required Text

Advanced Penetration Testing: Hacking the World's Most Secure Networks by Will Allsopp, ISBN-13: 978-1119367680 , ISBN-10: 1119367689

Other Materials

Penetration Testing Essentials 1st Edition by Sean-Philip Oriyano, ISBN-13: 978-1119235309 ISBN-10: 1119235308

Alfred Menezes, Paul van Oorschot, Scott Vanstone, Handbook of Applied Cryptography, CRC Press; 1 edition (October 16, 1996), ISBN-10: 0849385237/ISBN-13: 978-0849385230

The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition, Dafydd Stuttard ISBN-13: 978-1118026472 ISBN-10: 1118026470

Course Requirements / Due Dates

Interim Examinations

There will be two exams, midterm and final exams.

Homework Assignments

Homework problems will be assigned regularly and must be completed individually.

Class Projects

Class Projects are done in teams and focus on specific objectives.

Late Submission Policy

No Late submission will be accepted

Attendance Policy

Missing more than 3 classes will result in a 10 points reduction from your final grade.

Grading Policy

Activity	Points
Attendance and Participation	10
Midterm Exam	25
Homework Assignments	20
Class Projects	20
Final Exam	25
Total	100

Course grades are awarded based on the following scheme:

Score	Letter Grade
>= 90	A
>= 80 & < 90	B
>= 70 & < 80	C
>= 60 & < 70	D
< 60	F

Course Schedule

This is the list of topics. This could be adjusted as the semester progresses at the discretion of the instructor. Lecture slides will be posted to MUOline.

Week	Schedule
1	Introduction to Course
2	Introduction to Penetration Testing Concepts
3	Penetration Testing Scoping and Rules of Engagement
4	Online Reconnaissance and Offensive Counterintelligence
5	Social Engineering
6	Network Mapping and Scanning Techniques
7	Midterm Exam
8	Enterprise Vulnerability Scanning
9	Network Exploitation Tools and Techniques
10	Web Application Exploitation Tools and Techniques
11	Post-Exploitation and Pivoting
12	OS and Application Exploit Mitigations
13	Malware Analysis
14	Malware Locations and Footprints
15	Manual Code Reversing