Agenda Item #15-26
Effective: Spring 2017

Eastern Illinois University

New/Revised Course Proposal Format

(Approved by CAA on 4/3/14 and CGS on 4/15/14, Effective Fall 2014)

Banner/Catalog Information (Coversheet)

1. **__X_New Course or _____Revision of Existing Course**
2. **Course prefix and number:** _MIS 4860_____
3. **Short title:** _Ethical Hacking_____
4. **Long title:** _Ethical Hacking and Network Defense_____
5. **Hours per week:** _3_ Class _0_ Lab _3_ Credit
6. **Terms:** ___ Fall ___ Spring ___ Summer _X_ On demand
7. **Initial term**: ___ Fall _X_ Spring ___ Summer Year: _2017_
8. **Catalog course description:** Study of the techniques and the methods of ethical hacking, security testing, and network defense. Students gain experience with the tools and techniques used by security professionals in order to locate and fix vulnerabilities in companies' network defenses.
9. **Course attributes:**

   General education component: _____N/A_____

   ___ Cultural diversity ___ Honors ___ Writing centered ___ Writing intensive ___Writing active
10. **Instructional delivery**
    Type of Course:

    _X_ Lecture ___ Lab ___ Lecture/lab combined ___ Independent study/research

    ___ Internship ___ Performance ___ Practicum/clinical ___ Other, specify: _____

    Mode(s) of Delivery:

    _X_ Face to Face _X_ Online ___ Study Abroad

    _X_ Hybrid, specify approximate amount of on-line and face-to-face instruction: A maximum of 49% of the course will be online.
11. **Course(s) to be deleted from the catalog once this course is approved.** ____None_____
12. **Equivalent course(s):** _____None_____

    a. Are students allowed to take equivalent course(s) for credit? ___ Yes _X_ No
13. **Prerequisite(s): ____** BUS 3500 or permission of the Associate Chair.__

    a. Can prerequisite be taken concurrently? ___ Yes _X_ No

b. Minimum grade required for the prerequisite course(s)? _C_

c. Use Banner coding to enforce prerequisite course(s)? _X_ Yes ___ No

d. Who may waive prerequisite(s)?

___ No one ___ Chair ___ Instructor ___ Advisor _X_ Other (specify): Associate Chair

14. Co-requisite(s): _____None_____

15. Enrollment restrictions

a. Degrees, colleges, majors, levels, classes which <u>may</u> take the course: ___ALL_____

b. Degrees, colleges, majors, levels, classes which may <u>not</u> take the course: __NONE_____

16. Repeat status: _X_ May not be repeated ___ May be repeated once with credit

17. Enter the limit, if any, on hours which may be applied to a major or minor: _3_

18. Grading methods: _X_ Standard ___ CR/NC __ Audit ___ ABC/NC

19. Special grading provisions:

___ Grade for course will <u>not</u> count in a student's grade point average.

___ Grade for course will <u>not</u> count in hours toward graduation.

___ Grade for course will be removed from GPA if student already has credit for or is registered in: _____

___ Credit hours for course will be removed from student's hours toward graduation if student already has credit for or is registered in: _____

20. Additional costs to students:
Supplemental Materials or Software_____NONE_____

Course Fee _X_No ___Yes, Explain if yes_____

21. Community college transfer:

___ A community college course may be judged equivalent.

_X_ A community college may <u>not</u> be judged equivalent.

Note: Upper division credit (3000+) will <u>not</u> be granted for a community college course, even if the content is judged to be equivalent.

Rationale, Justifications, and Assurances (Part I)

1. _X_Course is required for the major(s) of _Master of Science in Cybersecurity (pending approval)_

   ___Course is required for the minor(s) of _____

   ___Course is required for the certificate program(s) of _____

   _X_ Course is used as an elective

2. **Rationale for proposal**: Ethical hacking is a legitimate, company-sanctioned approach through which ethical hackers locate and fix vulnerabilities in companies' network defenses. Many companies and government agencies seek professionals who have earned the Certified Ethical Hacker (CEH) credential or similarly skilled professionals to improve the security of their systems. This class was offered as a special topic in 2010. It was well received with all 32 open seats filled. With cybersecurity-related jobs being among the fastest growing jobs according to the 2014 U.S. Department of Labor's Occupational Outlook Handbook, this class will help prepare our students for those employment opportunities. MIS students who have successfully taken both MIS 4850 Systems Security and this class will be well prepared for a career in the cybersecurity field. This course will also be a required core course in an interdisciplinary Master of Science in Cybersecurity which is currently being developed.

3. **Justifications for (answer N/A if not applicable)**

   Similarity to other courses: N/A

   Prerequisites: Students enrolled in this class must have a good understanding of information systems and network operation. As a result, successful completion of BUS 3500 is necessary.

   Co-requisites: NONE

   Enrollment restrictions: N/A

   Writing active, intensive, centered: N/A

4. **General education assurances (answer N/A if not applicable)**

   General education component: N/A

   Curriculum: N/A

   Instruction: N/A

   Assessment: N/A

5. **Online/Hybrid delivery justification & assurances (answer N/A if not applicable)**

   Online or hybrid delivery justification: This course will be required in the Online Master of Science in Cybersecurity. Offering and instructing this course through a hybrid or online model also allows and increases the enrollment probability of students in the Summer semester who have moved away from campus and may attempt an equivalent course at another institution. An online course gives EIU the opportunity to market to these students as well as other students interested in taking the course in an alternative format. EIU School of Business continues to deliver high quality education through traditional methods of teaching and technologically advanced methods such as online and hybrid education. Students are able to watch recorded videos whenever they prefer, stop the video, take notes and ask questions

of the instructor and their peers. Ethical Hacking and Network Defense content is suitable for online or hybrid education.

Instruction: Lectures from the face-to-face courses may be recorded and posted online for students to view. Other online components (e.g., tutorials, videos, discussions) will be included. All faculty who will deliver this course online are/will be OCDI (or appropriate equivalent) trained.

Integrity: Students will take exams through an online testing taking monitoring system, or they will take them at a proctored facility such as a community college in their area.

Interaction: At the discretion of the faculty, provisions and requirements would vary but generally will utilize Email, Web-Based Discussions, and Web-conferencing.

Model Syllabus (Part II)

Please include the following information:

1. Course number and title
MIS 4860 Ethical Hacking and Network Defense

2. Catalog description
Study of the techniques and the methods of ethical hacking, security testing, and network defense. Students gain experience with the tools and techniques used by security professionals in order to locate and fix vulnerabilities in companies' network defense.

3. Learning objectives.
Upon successful completion of the course, students will be able to:

1. Analyze current corporate computer security threats. (CT 1-4), (Graduate 1,2)
2. Explain penetration and security testing issues. (WCR 1-3), (Graduate 1,2)
3. Analyze information security countermeasures. (CT 1-4), (Graduate 1,2)
4. Explain legal issues relating to ethical hacking. (WCR 1-3), (Graduate 1,2)
5. Perform security audits and security testing. (RC 1-4), (Graduate 1,2)
6. Conduct ethical hacking in a controlled environment. (RC 1-4), (Graduate 1,2)
7. Implement network defense measures. (QR 1-6), (Graduate 1,2)
8. Evaluate information security threats associated with computer networks. (CT 1-4), (Graduate 1,2)
9. Evaluate information security countermeasures. (CR 5-6), (Graduate 1,2)

4. Course materials.
- *Hands-on Ethical Hacking and Network Defense*, by Michael T. Simpson, Kent Backman, James Corley, 2nd edition, Cengage Learning, 2011, ISBN-13: 9781435486096
- Current academic literature on information security and ethical hacking such as:
    - Chickowski, E. (2013), The Future of Web Authentication, *Security Dark Reading*, May 2013 Issue, 1-11.
    - Lee, H., Zhang, Y., Chen K. (2013), An Investigation of Features and Security in Mobile Banking Strategy, *Journal of International Technology and Information Management*, 22(4), 23-45

5. Weekly outline of content.

Week	Topic	**75-minute class period equivalents**
1	Introduction to Ethical Hacking and Network Defense	2 periods
2	TCP/IP concepts	2 periods
3	Legal issues and network attacks	2 periods
4	Social engineering and footprinting	2 periods
5	Port scanning	2 periods
6	Enumeration	2 periods
7,8	Programming for security professionals	4 periods
9	Microsoft operating systems vulnerabilities	2 periods
10	UNIX/Linux operating systems vulnerabilities	2 periods
11	Hacking Web servers	2 periods
12	Hacking wireless networks	2 periods
13, 14	Cryptography	4 periods
15	Protecting networks with security devices	2 periods
16	Final Exam	2 hours
	Total	**Thirty 75-minute periods + Two hours of final exam**

6. Assignments and evaluation, including weights for final course grade.

Grade weighting may vary by instructor, but it is generally considered as follows:

Undergraduates:

- Exams (40% of total grade)
- Assignments (30% of total grade)
- Project/Case Study on current Information Security issues (15% of total grade)

  Sample Project/Case Study: In a controlled environment, students will use skills and techniques learned in class in order to analyze a network's vulnerabilities and write a report that details and explains their discoveries.
- Final Exam (15% of total grade)

Graduates

- Exams (40% of total grade)
- Assignments (20% of total grade)
- Research Project (25% of total grade)

  Sample Research Project: In a controlled environment, students will use skills and techniques learned in class in order to analyze a network's vulnerabilities. Furthermore, they will search academic and professional literature in order to write a research paper describing the vulnerabilities discovered in detail, providing a theoretical background about the vulnerabilities, and proposing an information security framework that can be adopted to effectively monitor and protect corporate networks against the discovered vulnerabilities.
- Final Exam (15% of total grade)

7. Grading scale.

90% or better	A
80-89%	B
70-79%	C
60-69%	D
Less than 60%	F

8. Correlation of learning objectives to assignments and evaluation.
The students' achievement of the stated course objectives will be assessed as follow:

Objectives	**Exams**	**Assignments**	**Project/Case Study**	**Final**
1	X	X		X
2	X	X	X	X
3	X	X	X	X
4	X		X	X
5	X			X
6	X	X		X
7	X	X		X
8	X		X	X
9	X	X	X	X

Date approved by the discipline: MIS/OM Discipline 2/3/2015
Date approved by the department or school: School of Business Graduate Committee 2/17/2015
Date approved by the department or school: School of Business Curriculum Committee 3/4/2015
Date approved by the college curriculum committee: LCBAS Curriculum Committee 4/8/2015
Date approved by the Honors Council ***(if this is an honors course):***
Date approved by CAA: CGS: