



## COURSE SYLLABUS

### Course Name: IA 543: Systems Operating Environment for Information Security Systems Administrators

Instructor: \_\_\_\_\_

Office Hours: \_\_\_\_\_

Office: \_\_\_\_\_ Telephone: \_\_\_\_\_ FAX Number: \_\_\_\_\_

Internet/E-Mail Address: \_\_\_\_\_

---

**Opening Statement:** This document is meant to serve as an information statement for your reading and use for this course. It also serves to identify timelines, requirements etc. The instructor reserves the right to make any additions/deletions or changes to this document or course as deemed necessary.

**Course Description:** Discusses specific information security technical defenses including operating system security, network security, infrastructure protection, approaches to protecting against viruses and rogue code, firewalls, identification and authentication, and encryption and public key infrastructure (PKI). Concepts such as quality assurance in an information security environment, anti-piracy techniques, security architecture development, Internet-facing system security and safeguards for eCommerce are also important parts of this course.

**Course Prerequisites/Corequisites:** IA 344

**Course Objectives:** Upon successful completion of this course, students should be able to:

1. Demonstrate understanding of MS Windows and Unix (including Linux) operating environments
2. Demonstrate understanding of the e-business security environment
3. Demonstrate understanding of security tools such as firewalls, intrusion detection systems, public key infrastructure (PKI), and antivirus safeguards
4. Demonstrate familiarity with types of hacking attacks, hacking tools and hacking techniques
5. Demonstrate understanding of network environments and protocols including local area networks (LANs), wide area networks (WANs) and the Internet
6. Demonstrate understanding of information security countermeasures and safeguards

#### Student Requirements:

**Text and Handouts:** Students will receive reading assignments that may include handout material, and/or research searches, and are responsible to read and act on the material as directed.

- Primary Text: Computer Security Handbook, fourth edition ed. Bosworth, Seymour, Kabay, M. E. pub. Wiley, Part 3 (Required text for the entire MLS/IS program)
- Supplementary text: Enterprise Security – the Manager’s Defense Guide Clark, David Leon pub Addison Wesley, Part 3 (Required supplementary text for the entire MLS/IS program)
- Complementary text: Securing E-Business Systems – A Guide for Managers and Executives Braithwaite, Timothy pub Wiley
- Various handouts as determined by your instructor

**Assessment and Evaluation:** The final grade for the class will be based on the following requirements as directed by your instructor:

- Team based development, presentation and evaluation of a final project, including a complete bibliography, and areas of further research will account for 40% of each student's grade.
- Student participation in class activities and individual assignments will account for 20% of the student's grade.
- Mid term and final exams will account for 20% each of the student's grade

All points are cumulated, converted to percent form, and converted to letter grades based on this straight scale: 94% and above, A; 90% and above A-; 87% and above, B+; 84% and above, B; 80% and above, B-; 77% and above, C+; 74% and above, C; 70% and above, C-; 67% and above, D+; 64% and above, D; 60% and above, D-; below 60%, E.

**Notes on Requirements and Grading:**

- Class sessions will involve interactive approach and student activities. Students are expected to have textbooks and other assigned materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, or other misc. materials including disks, or backup files (in case a file is lost or damaged).

**Attendance at all times is required of all students, and failure to attend is considered lack of participation. Verifiable emergencies will only be considered.**

**General Policies:**

- Attendance and punctuality is mandatory. Class will start at the given time.
- All cell phones, pagers and any other miscellaneous forms of communication must be turned off prior to the start of class and remain turned off until after class is completed. This is out of courtesy for the other students and to insure an un-interrupted class.
- Speak to the instructor as needed.
- Students should comply with expectations for use of the college and university laboratories and classrooms, with standards for fair information practices, and with licensing provisions of the software in use.
- Students must complete their own work when given an individual assignment. During team-based assignments they will work with one another to solve problems and develop the team-based project. Students who submit the work of other students, including companies and organizations, as their own (Plagiarism), will be penalized to the full extent permitted by University policy.
- Late work is not accepted. Oral presentations may not be made up.
- Inability to prepare for an assignment and poor time management are not considered valid reasons for late work or re-scheduling. In addition, students must back up work, for lost disks or damaged files is not sufficient reason for extensions.
- Class sessions may involve some lecture, Caucus/Online, with mostly group-facilitated activities. Therefore, it is the student's responsibility to have completed the scheduled reading assignment prior to the class session. The student must also complete the assigned chapter activities/projects during scheduled class sessions. Active listening is also part of learning. Students are expected to have textbooks and other needed materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, and/or other materials.
- Be prepared to conduct discussions online through Caucus or another form of online viewing such as e-mail.
- Students are expected to complete all assignments in a neat, accurate and professional manner; otherwise, materials will not be accepted. This includes the word processing of all assignments with spell checking and proofreading mandatory. This also includes stapling your materials if needed so they do not become loose.

- All assignments will be graded for compliance to the author's directions.
- Final grades will not be given in person, by telephone, e-mail, fax or any other communications median except that of University standard written grading at the end of the semester.
- Attendance/participation is required therefore it is the student's responsibility to obtain all missed instruction from another class member. The instructor will not repeat instructions or demonstrations for any student missing class. Keep in mind that attendance is mandatory.
- A grade of "I" will be given only in accordance with Eastern Michigan University's Graduate school guideline.
- By University policy the instructor has the option of failing a student who does not attend class on the day of the final examination set by the university. Attendance at final periods during which students are presenting their work is required of all students and failure to attend is considered lack of participation.

**Course Content and Schedule:** This schedule is an approximate timeline for the student.

**Week 1**

- **Introductions**
- **Course Review and Intro**
- **The foundations of e-business and e-commerce**
- **Security models and frameworks**

**Week 2**

- **Components of a secure e-business environment**
- **The concept of security policy domains**
- **Developing an information security architecture**

**Week 3**

- **Project and Team Selection**
- **Network technologies and protocols**

**Week 4**

- **Cyber attack tools and techniques**
- **Attack trees, introduction to attack detection and analysis**

**Week 5**

- **E-business security defenses and tools**
- **Public key infrastructure (PKI) and certificates**

**Week 6**

- **Intrusion detection system architectures**
- **Attack analysis**
- **Advanced attack techniques: firewalking, tunneling, etc.**

**Week 7**

- **Mid Term Exam**

**Week 8**

- **Firewall and proxy server architectures**
- **Analyzing attacks against firewalls**

**Week 9**

- **Stealth attacks and probes**

- **Introduction to forensic analysis**

**Week 10**

- **Conducting incident post mortems**

**Week 11**

- **Piracy defenses**
- **Software development and quality assurance in the information security environment**

**Week 12**

- **Testing web applications**
- **Using the Common Criteria as a guideline for information security safeguards**

**Week 13**

- **Project Work Session**

**Week 14**

- **Team Project Presentations and Business documents turned in.**  
\*\*\*No late projects or presentations will be accepted.

**Week 15**

- **Final Exam**

**Overview of the Semester Project:**

**Grading:** There are 40 points for the semester project and presentation.

There are 60 points for participation in class activities, assignments and exams.

The final project will be developed in teams with a team leader giving an oral presentation of the project to the class. Each student will write a portion of the team report and will be responsible for his or her contribution to the overall project. Each team will provide a final written team report with each team member's contribution identified individually.

**More on Planning the Project:**

Each team will develop a word processed business document, **completed in APA or MLA format**, which will be presented using PowerPoint and will at minimum include the following:

- Cover page with all Team Members Names, etc.
- Table of contents
- Names of Team members and their individual responsibilities
- The Team Leader is responsible for submitting each team member's participation and contributions to the project, which is to be included in the final document package.
- Statement of the problem. What are the issues you are dealing with and why.
- Summary statement focusing on the organization.
- Solution Statement: How will you deal with the problems, issues, etc.
- Bibliography
- Areas of further research, including a preliminary research proposal on a significant information security problem related to Systems Auditing.

The focus of the final project will be determined at the start of each term.

