MIS 5213 – Intrusion Detection and Response

Instructor Information	**Deval Shah**
Office Information	(609) 923-5912
Office Hours	Per Appointment or 5:00 – 5:30 Prior to class or After class.
Class	MIS.5213.011 ALTER 0A234 Monday 5:30 – 8:25 / Wednesday 5:30 – 8:25

Course Objectives

Firewalls are no longer sufficient to prevent intrusions. In the era of zero day exploits and increased level cyber threats, if an organization gets attacked in no longer as an option, but simply a matter of when. Is the organization ready and prepared for the next attack?

In this course you will learn what it takes to be prepared for that intrusion, what it takes to detect the intrusion, and eradicate it.

Key topics are:

1. Introduction of Intrusion Detection & Protection, and Incident Response Concepts
2. Familiarity with common IPS, IDS and IR approaches and their applications
3. Understanding of practical aspects of implementing and managing Intrusion Protection, Detection Systems
4. Familiarity with the Operations of effective Incident Response Processes and Organizations

Grading

Item	Percent of Total
Participation	25%
Term Paper	25%
Quizzes	25%
Exams	25%
Total	**100%**

MIS 5213 – Intrusion Detection and Response

Course Schedule

Date	Lecture Topic	Assignment / Activity	Reading
5/9/2016	Intro to Intrusion Detection / Response & Cyber Security Threat Landscape		Chapters 1 - 3
5/11/2016	Developing CIRT (Teams, Members, Roles, Responsibilities), Process Procedures, Policies		
5/16/2016	IDS (Signature, Anomaly, Network and Host) IDS	WEEK Preparation Submission (5.0%) / Quiz 1 (6.25%)	Introduction to Intrusion Detection and Prevention Systems (NIST SP 800-94, Network IDS and IPS Deployment Strategies, by Nicholas Pappas Using IOCs in Malware Forensics by Hun-Ya Lock Chapters 4 - 5
5/18/2016	Install Wireshark, Install Snort.		https://www.youtube.com/watch?v=l2w-fbyy6y0 https://www.youtube.com/watch?v=RUmYojxy3Xw
5/23/2016	Detecting Intrusions	WEEK Preparation Submission (5.0%)	
5/25/2016	LOG Management, Sys Log commands,	Quiz 2 (6.25%)	Chapter 10 – Chapter 12
5/30/2016	School Closed Memorial day		
6/1/2016	Install Splunk , Integrate logs from various area.	Week Preparation Submission (5%) Hands On Assignment – (6.25%)	
6/6/2016	Computer Forensics	WEEK Preparation Submission (5.0%) / Quiz 3 (6.25%)	Chapter 8 – Chapter 9
6/8/2016	Computer Forensics Tools		
6/13/2016	Intrusion Detection in an outsourced environments	Week Preparation Submission (5%)	
6/15/2016	FINAL EXAM	Final Exam (25%)	

Student Evaluation

1. Participation

Much of your learning will occur as you prepare for and participate in discussions about the course material. The assignments, cases, and readings have has been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts.

To encourage participation, 25% of the course grade is earned by preparing before class and discussing the topics between and in class. Evaluation is based on you consistently demonstrating your engagement with the material. Assessment is based on what you contribute, not simply what you know.

1) ***Preparation before class*** – By Sunday midnight, you will send me a brief (1 page) summary of the readings, including the cases, assigned for the upcoming class period (see the course schedule). Bring a copy for your reference during the discussion.

   Your weekly summary will briefly address and summarize:

   a. One key point you took from each assigned reading including the case. (One or two sentences per reading maximum)
   b. One key point you learned from the readings as a whole. (One or two sentences maximum)
   c. One question that you would ask your fellow classmates that facilitates discussion.

2) **Participation during class** – We will typically start each discussion with "opening" questions about the assigned readings and case study. I may ask for volunteers, or I may call on you. Students called on to answer should be able to summarize the key issues, opportunities, and challenges in the case study. All students should be prepared to answer these questions.

   Another important aspect of in-class participation is completion of in-class assignments and contribution to break out activities.

3) **Participation between classes** – To facilitate ongoing learning of the course material, we will also discuss course material on the class blog in between class. Please ask any questions about the readings or cases on the blog so all can see the answers. Reading and commenting by all on these post will further the quality of our in-class discussions.

   Also, I have posted discussion question about each week's cases on the class blog. The questions are meant to guide your reading and understanding of the case. Take notes and come to class prepared to discuss the case.

4) **Activities** – To facilitate ongoing learning of the course material, we will conduct classroom activities. Activities may require the use of your laptops to install security tools and use these tools. In addition, you may be required to conduct these activities on your own as homework assignment.

The criteria for participation includes attendance, punctuality, level of preparation, professionalism, answering questions, discussing readings, discussing case studies, contributing to group activities, and contributing to a positive learning environment. Recognizing that students sometimes have unavoidable conflicts, the baseline for expected participation is assessed on one less week than the number of

2. Term Paper

Intrusion Detection and Management comprises of several phases. Each phase consists of its own issues. Following are some of the examples and issues that need to be considered. Please pick one

of the following as your topic of the paper.

- Legal issues with the use of IDS Logs and Packet Capture Data.
- Financial Implications of not having an Intrusion Detection and Management program.
- Technical Obstacles with the deployment of IDS
- Effectiveness of Intrusion Detective Systems
- Pros and Cons of sharing the details of a cyber-attack with the government or other entities.
- Identify several metrics that you would consider developing to highlight the success of a Cyber Incident Security Response Centers.

All papers need to have the following requirements.

- APA formatting,
- A minimum of 5 professional references (Def: professional references are those that have been published in journals or industry publications. Websites and Blogs will not be considered professional references)
- A minimum of 10 pages but no more 12 pages.

3. Quizzes

There will be a quiz that covers the topics discussed the previous week. The quizzes will consist of seven to ten questions.

4. Final Exam

The final exam will use all multiple-choice, multiple answer, short essay, and quick analysis type questions. Value of each question will be weighted on the difficulty and the complexity of the question. The final exam consists of 50 questions.

Grading Criteria

The following are the criteria used for evaluating assignments. You can roughly translate a letter grade as the midpoint in the scale (for example, an A- equates to a 91.5).

Criteria	Grade
The assignment consistently exceeds expectations. It demonstrates originality of thought and creativity throughout. Beyond completing all of the required elements, new concepts and ideas are detailed that transcend general discussions along similar topic areas. There are few mechanical, grammatical, or organization issues that detract from the ideas.	A- or A
The assignment consistently meets expectations. It contains all the information prescribed for the assignment and demonstrates a command of the subject matter. There is sufficient detail to cover the subject completely but not too much as to be distracting. There may be some procedural issues, such as grammar or organizational challenges, but these do not significantly detract from the intended assignment goals.	B-, B, B+
The assignment fails to consistently meet expectations. That is, the assignment is complete but contains problems that detract from the intended goals. These issues may be relating to content detail, be grammatical, or be a general lack of clarity. Other problems might include not fully following assignment directions.	C-, C, C+
The assignment constantly fails to meet expectations. It is incomplete or in some other way consistently fails to demonstrate a firm grasp of the assigned material.	Below C-

Plagiarism, Academic Dishonesty and Citation Guidelines

If you use text, figures, and data in reports that was created by others you must identify the source and clearly differentiate your work from the material that you are referencing. If you fail to do so you are plagiarizing. There are many different acceptable formats that you can use to cite the work of others (see some of the resources below). The formats are not as important as the intent. You must clearly show the reader what is your work and what is a reference to somebody else's work.

Plagiarism is a serious offence and could lead to reduced or failing grades and/or expulsion from the university. The Temple University Student Code of Conduct specifically prohibits plagiarism (see http://www.temple.edu/assistance/udc/coc.htm).

The following excerpt defines plagiarism:

Plagiarism is the unacknowledged use of another person's labor, ideas, words, or assistance. Normally, all work done for courses — papers, examinations, homework exercises, laboratory reports, oral presentations — is expected to be the individual effort of the student presenting the work. There are many forms of plagiarism: repeating another person's sentence as your own, adopting a particularly apt phrase as your own, paraphrasing someone else's argument as your own, or even presenting someone else's line of thinking in the development of a thesis as though it were your own. All these forms of plagiarism are prohibited both by the traditional principles of academic honesty and by the regulations of Temple University. Our education and our research encourage us to explore and use the ideas of others, and as writers we will frequently want to use the ideas and even the words of others. It is perfectly acceptable to do so; but we must never submit someone else's work as if it were our own, rather we must give appropriate credit to the originator.

Source: Temple University Graduate Bulletin, 2000-2001. University Regulations, Other Policies, Academic Honesty. Available online at: http://www.temple.edu/gradbulletin/

- For a more detailed description of plagiarism:
- Princeton University Writing Center on Plagiarism:
- http://web.princeton.edu/sites/writing/Writing_Center/WCWritingRes.htm
- How to successfully quote and reference material:
- University of Wisconsin Writers Handbook
- http://www.wisc.edu/writing/Handbook/QuotingSources.html
- How to cite electronic sources:
- Electronic Reference Formats Recommended by the American Psychological Association
- http://www.apastyle.org/elecmedia.html

Readings	
Text	**The Practice of Network Security Monitoring: Understanding Incident Detection and Response** by Bejtlich, Richard. **Incident Response & Computer Forensics, Third Edition** By Jason Luttgens, Matthew Pepe, Kevin Mandia

Other	**Network IDS and IPS Deployment Strategy** http://www.sans.org/reading-room/whitepapers/intrusion/network-ids-ips-deployment-strategies-2143
	Intrusion Kill Chains http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
	The Practice of Network Security Monitoring: Understanding Incident Detection and Response by Bejtlich, Richard.
	csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf