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 / MIS.5213.711 ALTER 0A745 Monday 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 / Due Dates	Percent of Total Points
Discussion Topics / Class Participation (weekly)	10%
Short Papers	15%
Term Paper	10%
Executive Brief - Presentation	5%
Quizzes	15%
Midterm	15%
Final	20%
LABS	10%
Total	**100%**

Student Evaluation

1. Participation / Discussion Topics (10%)

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, 10% of the course grade is earned by preparing, participating and contributing to class learning in the form of Discussion Topics questions and class activities. Evaluation is based on you consistently demonstrating your engagement with the material. Assessment is based on what you contribute, not simply what you know.

On a weekly basis, I will post a topic for discussion, students are also encouraged to post questions and topics for discussion. Students are than asked to contribute of interest in current events. Students should try to provide at least two responses, comments or rebuttals.

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 for a minimum of 8 weeks.

2. Short Papers (15%)

Students are expected to write three short papers in the form of executive summaries. The summary will review the main points of the topic assigned. The paper should succinctly discuss the impact or any recommendations if necessary.

Topic 1: "We are a small organization, a non- profit" why would we be hacked? **Due Date: 5/28/2017**
Topic 2: "What is our biggest threat? Why?" **Due Date: 6/11/2017**
Topic 3: "Am I violating privacy of my users when we monitor?" **Due Date: 7/23/2017**

All papers need to have the following requirements.

- APA formatting,
- A minimum of 2 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 3 pages but no more 4 pages.

3. Term Paper (10%)

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. **Due Date: 7/9/2017**

- 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.

4. Quizzes (15%)

There will be two quizzes. Quizzes will cover the topics not previously covered in either midterm or quiz.

Quiz 1: **5/31/2017**
Quiz 2: **7/17/2017**

5. Midterm: (15%) 6/19/2017

There will be Midterm which will cover the first half of the course

6. Final: (20%) 8/7/2017

There will be Midterm which will cover the first half of the course.

7. Executive Brief - Presentation (5%) 7/31/2017

Based on everything, creating a 12 slide deck that discusses your road map to building a SOC.

8. LABS: (10%)

There will be many labs throughout the course. A system with either Windows/Linux will be required. More importantly we will be installing Wireshark or other packet capture tool, along with Snort and Splunk. We will also install a network scanner on this device. So, make sure your important data is properly protected.

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, and 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	**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
	Building a World-Class Security Operations Center: A RoadMap https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907
	csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
	C-Level support for SOC https://www.sans.org/reading-room/whitepapers/analyst/c-level-support-ensure-high-impact-soc-rollout-37347
	SANS Reading: Successful Log and SIEM Strategies https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528

MIS 5213 – Intrusion Detection and Response

Schedule

Lecture	Date	Topic	Reading	WRITTEN ASSIGNMENTS	ACTIVITIES	EXAMS
1	5/15/2017	Introduction to Incident Response and Intrusion management	Luttgens: Chapters 1 & 2			
2	5/22/2017	CIRT	Luttgens: Chapters 3	Short Paper 1	Group Exercise: Components of CIRT	
3	5/31/2017	Wireshark / Packet Captures	https://www.youtube.com/watch?v=l2w-fbyy6y0 https://www.youtube.com/watch?v=RUmYojxy3Xw		Lab1: Install Wireshark Lab2: Extract Data Lab3: Analyze Malware Packets	**QUIZ 1**
4	6/5/2017	IDS/IPS	SANS Reading: Network IDS and IPS Deployment Strategies, by Nicholas Pappas	Short Paper 2		
5	6/12/2017	DETECTING INTRUSIONS	Luttgen: Chapters 4 - 5		LAB4: INSTALL AND CONFIGURE SNORT LAB5:CREATE RULES LAB6: DETECT ATTACKS	

6	6/19/2017	ESCALATION			ESCALATION TEST / EXECUTE PLAN	**MIDTERM**
	6/26/2017	**NO CLASS THIS WEEK**				
7	7/3/2017	LOGS / SIEM	SANS Reading: Successful Log and SIEM Strategies Luttgen: Chapters 10	TERM PAPER	Group Exercise: What to Log	
8	7/10/2017	LOGS / SIEM	Luttgen: Chapters 11 - 12			
9	7/17/2017	SPLUNK		Short Paper 3	LAB7: INSTALL SPLUNK LAB8: CONFIGURE SPLUNK LAB9: ANALYZE SPLUNK DATA	**QUIZ 2**
10	7/24/2017	SOC : How to build a SOC for Incident Response Center	World Class SOC C-Level support for SOC			
11	7/31/2017			Executive Brief: ROAD MAP TO BUILDING A SOC		
12	8/7/2017					**FINAL**