MSIS 5263: Information Assurance Offense
Spring Semester 2018

Sections:
MSIS 5263.26983

Instructor: Dr. Jim Burkman
E-mail: jim.burkman@okstate.edu
Office: GAB 311C / BUS 306
Office Hours: By appointment
Phone: 744-5142
Club: http://isac.okstate.edu

Textbooks: None required, but several books and resources helpful to pen testing will be recommended during the course.

Resources: I expect that you have administrative control of a laptop or desktop computer that has at least 8 GB of RAM and sufficient CPU power and disk space to allowing for running 2-3 virtual machines at once. We supply VMWare products for both Mac and Windows hosts. Inform me immediately if this presents a problem for you, though as a last-semester graduate IA student owning a decent computer is an inescapable necessity.

Peer Grading: We will use the CrowdGrader website for some of our coursework https://www.crowdgrader.org/. I will provide the specific assignment links as needed. You must sign up there with a google account that uses enough of your real name that I can easily identify you.

Discussion Forum: There is a discussion forum on Brightspace where you can share information, ask questions, etc. I'll be hanging out there as well.

The OSU Spring Syllabus Attachment includes important dates, information, and resources to HELP YOU SUCCEED and is available on the course Brightspace site.

Course Site: (Brightspace by D2L): http://online.okstate.edu or http://my.okstate.edu (choose Online Classroom after logging in)

Online Learning Support: spearsonline@okstate.edu
Phone: 405-744-4048
Facebook: Follow Spears School Online Learning on

Facebook! http://www.facebook.com/SpearsOnline/

Course Description: Cybersecurity is at the top of government and corporate agendas. Effective cybersecurity starts with understanding how vulnerabilities arise and how they are exploited. You can't play defense if you don't understand what the offense is doing. This course is one of the final ones within the OSU MSIS Department's graduate IA curriculum and you will be expected to demonstrate professional presentation and mastery of the topics.

The course material is organized into four themes: Passive Discovery, Active Discovery, Exploitation, and Post-Exploitation. Planning, Reporting and Mitigation will also be integrated into the course.

Course content will be delivered primarily through online lectures and demonstrations, and may be augmented with additional assigned reading and videos.

Due to the nature of this class you will be held to the highest ethical standards. Be sure to ask if you have any questions about the safety of a project or demonstration that you are planning.

This course will require a significant amount of your time and effort. Budgeting at least 10 hours a week for this course (as an average) is not an unrealistic idea. Ultimately, the test of every submission in this class will rest on a foundational metric of "is this a strong graduate/professional submission that demonstrates effort and subject mastery?" Half-measures and last minute products will not see you through this course.

Be sure to check the Brightspace site often. This syllabus and the content on the Brightspace site for this class will likely change in response to the progress of this class. The policies and schedule in this syllabus are subject to change at my discretion, upon notice in any form to the class. Changes to the syllabus will be posted on Brightspace as a new syllabus with v1, v2, etc.

You are responsible for getting any downloads offered for upcoming classes from Brightspace. Handouts, assignments, slides, due dates, and other information will be posted on Brightspace, and peer graded will be done on CrowdGrader.

Learning Goals and Course Objectives:

Information Assurance Competence

Upon completion of this course the student should be able to:

Identify the ethical issues related to professional penetration testing.

Illustrate the necessary components of a pen testing agreement and reference applicable local, state and federal laws.

Demonstrate mastery of IA concepts, both in theory and in practice.

Communication Skills

Upon completion of this course the student should be able to:

Effectively prepare a comprehensive, efficient knowledge repository for future use as an IA professional.

Create written and video tutorials and examples that effectively teach technology tool usage to relevant others.

Clearly explain specific vulnerabilities, exploits and controls to people of widely varying skill sets.

Technological Competence

Upon completion of this course the student should be able to:

Recognize, discuss and evaluate a variety of core MIS technical skills including (but not limited to): hardware, software and network configurations; basics of application development; open vs closed source software; selecting and using hardware and software to achieve specific goals.

Identify and locate vulnerabilities in a variety of environments. Use applications and tools offensively against networks, computing devices and other applications to exploit those vulnerabilities. Suggestion broad and specific controls to counter the vulnerabilities.

Attendance: Attendance is at your whim, given that this is an online course. The coursework will be substantial, however, and assignment deadlines are immutable. I suggest that you stay very involved and very on top of this course.

Participation: Class participation is an integral part of the class. It includes not only your ability to read assigned class materials but also your ability to scan the environment and contribute scholarly information that you find. Feel free to email me your thoughts and questions and/or share them on the forums! Also, please stay up on current information security events. Helping each other out on the forums is a good idea (though everyone must do their own work).

Class Conduct: In the course forums and all correspondence please always keep your comments civil. No trolling, no passive-aggressive snarking.

Graduate Grading:

Weekly Assignments (RER)	47%
Tutorials (4 @ 9% each)	36%
Knowledge Repository (KR)	17%

A course grade of 90% or better will result in a letter grade of A, 80-89% B, 70-79% C, 60-69% D, <60% F. **NOTE!** I reserve the right to uniformly move the class average up at the end of the semester. For example, if the course average is 70%, I will not move it to 68%, but I may move it to 72%. This is not a curving process, as all individual scores would move the same amount.

Exams: This class has no exams.

Weekly Assignments (RER): Most weeks (typically about 11 weeks out of the semester) you will be tasked to Repeat, Extended, and Report (RER). An RER assignment will require you to repeat my demonstration in a way that is verifiably your own work, extend one or more tools to a different environment or usage, and report on both the repeat and the extend, along with a write up on the vulnerability(ies) and relevant control(s). Specific details will be provided on Brightspace and are considered to be part of this syllabus. All RER will be weighted equally regardless of content and are collectively worth 47% of the course grade. Unless stated otherwise, RER assignments will be due by 8 am CST on the Monday after I assign the RER.

Tutorials: After each major course section (Passive Discovery, Active Discovery, Exploitation and Post-Exploitation) you will be responsible for the creation of a written tutorial and video demonstration of a tool that was either not covered in the course or is used in a significantly different manner or environment than provided in the course. Tutorials are expected to be highly professional and demonstrate high proficiency with that tool. Tutorials will be peer graded.

Students must participate in peer grading (on time) to earn any credit for their own submission. Tutorial grades are subject to final adjustment by the instructor.

Be very aware of plagiarism when thinking about your tutorials. Your work must be independent and sufficiently unique so that it doesn't mimic any other tutorial on the internet or in any other resource. Specific details for each tutorial will be provided on Brightspace and are considered to be part of this syllabus.

Knowledge Repository: The Knowledge Repository (KR) is your main take-away from this course. Unlike the RER assignments that report on what you did, the KR is a comprehensive written resource built on a framework of your choice that provides all relevant information about every tool, every vulnerability, and every control used in this class. *This includes tools presented by other students in their tutorials.* The KR should be a massive, professional product that reflects a semester of work. Specific details for the KR will be provided on Brightspace, are likely to evolve over the course of the semester, and are considered to be part of this syllabus.

Software: Since you are enrolled in an MSIS class you will have access to our MSDNAA license and our VMWare license. You should receive an email with information about this opportunity. Go to Login, click on the "I forgot my password", and provide your Okey email as your login name. Your password will be mailed to you. Note that this can take a few days to get set up at the start of the semester. If you'd like to learn how to virtualize Windows on your Mac using this free software let me know and I'll help!

Instructor Response: You should hear back from me within the hour for most emails. If for some reason you've not gotten a response with 24 hours please email me again. That's a rare oversight on my part. Remember, emailing me is the fastest way to get my attention!

Make-up Policy: Students are expected to turn in each assignment on time. Late assignments are docked 1% per hour or fraction of an hour (62 minutes late = 2% penalty). Exceptions to deadlines will be extremely rare.

Drop Policy: Information about university drop policy and dates is at:
http://registrar.okstate.edu/
Click on "class schedules," and "short courses"
To drop this course, contact the Registrar's office, (405) 744-6876, or drop through Banner Service.

Academic Conduct: Oklahoma State University is committed to the maintenance of the highest standards of integrity and ethical conduct of its members. This level of ethical behavior and integrity will be maintained in this course. Participating in a behavior that violates academic integrity (e.g., unauthorized collaboration, plagiarism, multiple submissions, cheating on examinations, fabricating information, helping another person cheat, unauthorized advance access to examinations, altering or destroying the work of others, and fraudulently altering

academic records) will result in your being sanctioned. Violations may subject you to disciplinary action including the following: receiving a failing grade on an assignment, examination or course, receiving a notation of a violation of academic integrity on your transcript (F!), and being suspended from the University. You have the right to appeal the charge. Contact the Office of Academic Affairs, 101 Whitehurst, 405-744-5627, academicintegrity.okstate.edu.

Additionally, if you engage in unethical use of any computing resources during this class you may be subject to additional administrative penalties under the OSU Student Code of Conduct along with relevant local, state and/or federal statutes. This is a professional white-hat hacking course, not a license to play script kiddie on the internet.

Disabled Students: According to the ADA, each student with a disability is responsible for notifying the University of his/her disability and requesting accommodations. If you think you have a qualified disability and need classroom accommodations, contact the office of Student Disability Services (SU 315). Please advise the instructor of your disability as soon as possible, to ensure timely implementation of appropriate accommodations. Faculty have an obligation to respond when they receive official notice of a disability from SDS but are under no obligation to provide retroactive accommodations. To receive services, you must submit appropriate documentation and complete an intake process during which the existence of a qualified disability is verified and reasonable accommodations are identified. For more information about OSU Student Disability Services, please go to: http://sds.okstate.edu or call 405-744-7116 v/t.

Course Topics (Subject to Change)		
Week 1	Jan 15	OFF00/01 – Course Overview and Setup
Week 2	Jan 22	OFF02 - Frameworks
Week 3	Jan 29	OFF03 – Basic Tools
Week 4	Feb 5	OFF04 – OSINT I
Week 5	Feb 12	OFF05 – OSINT II
Week 6	Feb 19	**Tutorial/KR Passive Discovery (not scanning!)**
Week 7	Feb 26	OFF06 - Active Discovery I
Week 8	Mar 5	OFF 07 - Active Discovery II
Week 9	Mar 12	**Tutorial/KR Active Discovery**
Week 10	Mar 19	**Spring Break**
Week 11	Mar 26	OFF08 - Metasploitable
Week 12	Apr 2	OFF09 - another hack/maybe dodge av
Week 13	Apr 9	**Tutorial/KR Exploitation (getting in and dropping off)**
Week 14	Apr 16	OFF10 - Meterpreter
Week 15	Apr 23	OFF11 – Password Cracking
Week 16	Apr 30	**Tutorial/KR Post-Exploitation (finding things)**
• **Knowledge Resource is due on Monday of Final week, 8 am (CST)**		