CMNET 250 – Hybrid class – Class time is for lab and questions, lectures online (via Moodle)

ILLINOIS CENTRAL COLLEGE
COURSE SYLLABUS

A. DESCRIPTION

1. CMNET 250 – Advanced Security Topics

2. Prerequisite: CMNET 210 with a grade of "C" or better or departmental approval

3. This course is designed to teach the fundamentals of securing Windows servers that are connected to corporate networks and the Internet. In addition to learning the fundamentals of designing a secure framework, students will learn how to secure computers based on their function, how to secure the network management process, and how to configure group policies and administrative functions to increase ease of maintenance while retaining high levels of security. Students will learn the fundamentals of scripting with an emphasis on PowerShell™, how to use existing scripts to assist in rapid deployment of security fixes and documentation, how to write scripts to interface with the operating system, and how to document scripts so they can be maintained by others. Students will learn terminology associated with security, scripting, and the fundamentals of risk assessment and management.

4. This is a hybrid course. Two hours lecture hours (online) and two hours lab per week. Class meets once each week (**Wednesday** from **1:00** until **2:50** p.m. in **TC 310 – ICC East Peoria Campus**). You are expected to set-up a meeting with me, if you have received an unsatisfactory on 3 labs in a row or failed 3 quizzes in a row.

5. Credit: Three semester hours.

B. GENERAL EDUCATION GOALS

#7 – The student has the attitudes and skills required to function in a technological society.

C. OBJECTIVE

1. learn the fundamentals of securing Windows servers. (#7)

2. understand how to secure computers and networks based on their function. (#7)

3. learn the fundamentals of designing a secure framework. (#7)

4. learn the fundamentals of scripting as well as how to write and document scripts. (#7)

5. learn how to use existing scripts. (#7)

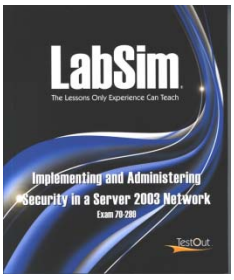
D. MATERIAL OF INSTRUCTION

CMNET 250 – Hybrid class – Class time is for lab and questions, lectures online (via Moodle)

1. **Text**: Liu, D. and R. Wisselink Securing Windows Server 2008: Prevent Attacks from Outside and Inside Your Organization, Syngress, Rockland, MA 2008. ISBN 978-1-59749-280-5. **Required text available from the ICC bookstore.**

2. **Text**: LabSim: Implementing and administering Security in a server 2003 Network. Test Out ISBN 978-1-935080-14-5. **Required text available from the ICC bookstore.**

   A note about LabSims. These can be installed on up to 3 computers (and **only 3** computers, for example, a home desktop computer, a lab computer at ICC, and a laptop). Once you register, this software will "phone home" periodically to synchronize. You will need to complete the simulations and the exams and turn in the completed scores at the end of the semester. You must complete all the lab simulations to receive a Satisfactory score. I will take the average of all the exams and factor that for your LabSim quiz score.



3. Instructor supplied materials, reference Web sites. This includes the free book – **Mastering Powershell** by Tobias Weltner. You can download it from here: http://www.c-sharpcorner.com/Resources/Detail.aspx?ResourceId=770

E. METHODS OF PRESENTATION

1. Lecture.
2. Class discussion.
3. Laboratory work.

F. METHODS OF ASSESSMENT OF STUDENT LEARNING

1. Periodic student surveys
2. Periodic Pre/ post test
3. Muddiest point
4. Weekly voting/ feedback regarding how well weekly material is understood.

G. EVALUATION OF STUDENT ACHIEVEMENT

- **Late work is not acceptable in this course. Unless you make prior arrangements, any assignments submitted after their due date will be ignored.**
- **Attendance confirmation requests -** In some cases, I am asked to provide a student's last date of attendance; for instance, in response to a request for this information from the financial aid and/or advisement departments. I will use the due date of the last completed graded quiz or attempted assignment to answer these requests.
- **Lab work (50%)** – Weekly laboratory performance to be completed the same night it is assigned. Successful weekly project completion of approximately 13 labs (LabSims will count for one lab) expected will count for your fifty percent. **Labs will be graded as either satisfactory or unsatisfactory. If a lab is unsatisfactory, you have 1 week to resubmit the lab. You can only resubmit any given lab once. I will not accept any work after the date it is due unless you make prior arrangements** – it is important all students keep up with the pace of this class. This means you must submit an "unsatisfactory" assignment to receive the week extension.
- **Blog entries (10%) –** Blog entries in the Moodle weblog will be required weekly and must include information from the appropriate chapter and lab work (eg. insights, problems encountered, web sites visited). **It will be your responsibility to keep this up to date each week. If your entry is not posted by the deadline your entry will receive a failing grade for that particular topic**. Don't try to do all the last week or two of class; each entry is time stamped.
- **Participation** – based on attendance, effort, and class participation. It is imperative that you participate fully in each class. If you miss 4 weeks out of the semester, your final grade will be lowered one letter grade (an "A" becomes a "B"). If you miss 6 weeks out of the semester, your final grade will be lowered 2 letter grades (an "A" becomes a "C"). If you miss more than 6 weeks out of the semester, I strongly recommend you drop the class.
- **Quizzes (30%)** – and three quizzes (10% each = 30%) –(**LabSim exams will count for one quiz – this is a significant part of your quiz grade**) note all quizzes may contain a hands on component, and
- **Final exam (10%)** – the final exam will be comprehensive (10%). Grades will be based on the following scale:

100 – 90%	**A**
89 – 80%	**B**
79 – 70%	**C**
69 – 60%	**D**
Below 59%	**F**

Hypothetical worked example to calculate a final grade:

Category	Grades	Average Score	Weight	Contribution
Labs	S, S, U, S, S, S, S, S, S,			

	U, S, U, S (LabSim completed)	10/13 = **76.9**	50%	**38.46**
Blog entries (Moodle)	S, S, U, S, S, S, U, S, S, S, S, S, U	10/13 = **76.9**	10%	**7.69**
Quizzes	65, 85, 78 (LabSim exams average)	228/ 3 = **76**	30%	**22.80**
Final	75	75	10%	**7.50**
		Overall	100%	**76.5% = C**

H. COURSE CONTENT (we will try to follow material in the order below). This schedule is tentative and may be adjusted as class proceeds. Please read each chapter before class so you are prepared. All students are expected to participate in class. Since this is a hybrid class, it is important to read the textbook chapters before coming to class. **Topics** correspond to topic headings in Moodle.

Week of	Topics for week	Read prior…
Key dates: **February 1, 2012 – refund date for this class** **April 7, 2012 – withdrawal date for this class**		
Topics 1 & 2 Jan. 18, 2012	• Course overview and review syllabus • Introduction to class and assessing need for security • **Lab 1**: Installation of Windows Server and updates and Virtual Environment • **Blog entry**	Liu Text – **Ch. 1** Instructor supplied materials
Topic 3 Jan. 25, 2012	• Scripting fundamentals and logic • **Lab 2:** PowerShell fundamentals and logic • **Blog entry**	Weltner Text – **Ch. 1, Ch. 2**
Topic 4 Feb. 1, 2012	• PowerShell variables, operators, expressions • **Lab 3:** Running PowerShell scripts • **Blog entry**	Weltner Text – **Ch. 3, Ch. 4**
Topic 5 Feb. 8, 2012	• PowerShell pipeline and objects • **Lab 4:** More advanced PowerShell scripts • **Blog entry** •	Weltner Text – **Ch. 5, Ch. 6**
Topic 6 Feb. 15, 2012	• PowerShell conditional expressions • **Lab 5:** Powershell script with choice • **Blog entry** • **Quiz 1 (through topic 4)**	Weltner Text – **Ch. 7**
Topic 7 Feb. 22, 2012	• PowerShell loops • **Lab 6**: PowerShell script with loop • **Blog entry**	Weltner Text – **Ch. 8**
Topic 8 Feb. 29, 2012	• PowerShell functions and scripts • **Lab 7:** PowerShell script using function	Weltner Text – **Ch. 9, Ch. 10**

	• **Blog entry**	
Drop for no attendance policy: **While I hope that everyone enjoys and completes the course, I want to make everyone aware of my withdrawal/drop for no attendance policies. At midterm, we are required to report to the state whether students are attending class or not. If you are not keeping pace with the class (no more than two assignments behind), I will report you as a non-attender. This means that you will be withdrawn from the course, and receive a grade of "W". You will not receive a refund. Therefore, if you are having difficulties in the course, or have circumstances come up that interfere with your course work but you would still like to try to complete the course, it is YOUR responsibility to contact me prior to midterm and let me know your status so I do not report you as a non-attender. The reverse is also true; if you are keeping pace with the class by midterm, I will NOT drop you from the course, which means that if you wish to withdraw from the course, you will need to do so before the withdrawal deadline listed in the ICC course schedule. There are no withdrawals allowed after the deadline date. Do not simply stop participating/turning in assignments-if you do not formally withdraw, you will receive a failing grade in the course.**		
Topic 9 Mar. 7, 2012	• PowerShell file handling • **Lab 8:** PowerShell file handling • **Blog entry** • **Quiz 2 (through topic 9)**	Weltner Text – **Ch. 15, Ch.16**
Mar. 14, 2012	• Spring Break	Enjoy!
Topic 10 Mar. 21, 2012	• Analyzing risk • **Lab 9:** Data destruction analysis • **Blog entry**	Instructor supplied materials
Topic 11 Mar. 28, 2012	• Developing a PKI • **Lab 10:** PKI • **Blog entry**	Liu Text – **Ch. 2**
Topic 12 Apr. 4, 2010	• Securing IIS and using MBSA • **Lab 11:** MBSA • **Blog entry**	Instructor supplied materials
Topic 13 Apr. 11, 2012	IIS Logfile analysis **Lab 12:** logfile analysis Note: You can withdraw only through the end of the 12th week of the semester and receive a grade of "W." **Blog entry** **Quiz 2 (through topic 12)**	Instructor supplied materials
Topic 14 Apr. 18, 2012	• Securing AD and Server Core and Terminal Services • **Lab 13**: securing AD and server core • **Blog entry**	Liu Text – **Ch. 3, Ch. 7, Ch. 9**
Topic 15	• Securing Virtualization and Hyper-V	Liu Text –**Ch. 8**

CMNET 250 – Hybrid class – Class time is for lab and questions, lectures online (via Moodle)

Apr. 25, 2012	• **Lab:** none	
Topic 16 May 2, 2012	• Review session (analyzing risks and emerging threats), PowerShell Administrative tasks • **Turn in printed copy of LabSim exercise scores** • **Turn in printed copy of LabSim examination scores** • **Lab:** none	Instructor supplied materials Weltner Text – **Ch. 17, Ch. 18, Ch. 19**
FINAL May 11, 2012	• ***Comprehensive Final Exam – you may take this online (it must be completed before May 11, 2012, 1:50 p.m.) or you may take it in person during the assigned time – Noon to 1:50 p.m. on May 11 in TC 310***	

Contact Information: Office Hours are posted on my web pages. I can be reached via e-mail (**mdubois@icc.edu)**. My web pages are located at: **http://blog.markdubois.info**

CMNET 250 Network Security
Additional Procedures which must be followed

General Guidelines:

1. Make every effort to complete each lab on the day it is handed out (**I will not accept late work unless you specifically arrange in advance**).

2. It is my continued intent to generate as little paper as possible. For labs, you will be asked to demonstrate in class that you have completed them successfully. If you are unable to do so, send me a series of screen captures (discuss with me prior to sending them so we decide upon the appropriate mechanism). Document what you do. It is likely some labs will build on prior work.

3. You are encouraged to maintain a high degree of professionalism in all your work.

Late Work:

1. Work is due on the dates assigned. Since much of this class builds from week to week, it is important to keep up with the class. The best method I have to verify your progress is successful completion of weekly labs and quizzes. **Again, no late work will be accepted unless you have made prior arrangements with me.**

2. If there are extenuating circumstances, such as illness or military service, business trips, and so on, special arrangements can be made only if you contact me, **in advance**.

3. Incomplete grades for the entire course are only given for extenuating circumstances (for example, you are very sick the week of the final). I would only accept the final or one other item to be turned in to satisfy an incomplete. Thus, if you become significantly behind in class, I encourage you to drop by the date listed in the syllabus. Otherwise, you risk receiving a grade of "F."

Criteria for Grading Work:

1. All lab materials and projects must conform to the rules outlined on that specific assignment.

2. Work must correctly answer questions or must clearly show that you completed the assignment.

3. If you are ever in doubt of what I am looking for, please ask before the work is due.

4. Work must be submitted in the proper format and on time **and must be original (see authorship section below)**.

Lecture/Lab Times (and attendance):

1. I will provide weekly materials for you to review. I will try to present an overall discussion of the necessary materials and present some additional information not available in the course text. Ask questions at any time if you do not understand something or are confused.

2. This material is not a substitute for reading and studying the text book! Always study the chapters fully before attempting the assignments. It helps to read the material before class (that is why the schedule is provided on this syllabus).

3. It is up to you to ask when you need help.

4. My attendance policy is that I expect you to actively participate in every class. This is the reason that your grade will be lowered should you miss certain classes.

Course Difficulty:

1. This course is designed as an intermediate course. As such, materials presented from class to class build upon each lecture/lab. If you are unable to participate in the majority of lectures and labs, you will not do well in the course. It is imperative to participate in discussions and to complete all assignments in the order they are presented and in the timeframe required.

2. It is expected that you will spend some time working on these assignments. We will be covering a lot of material during the semester and you are expected to keep up.

3. If you get confused or do not understand something ASK at once. I provide a number of means to contact me, please use them.

CMNET 250 – Hybrid class – Class time is for lab and questions, lectures online (via Moodle)

How to Succeed in the Course:

1. Participate in class discussions regularly, take notes, read and study the book, and ask questions when needed. When you find something that is not clear or not understood, make a note of it and ask me during my office hours or send me an email.

2. Stay on schedule as much as possible. Thoroughly learn each topic as when it is first assigned. All the rest of the course depends on your understanding each topic in sequence. There is no time for you to go back at a later date and learn it again (do it the first time). The better you know the current material, the easier it will be to understand the next topic.

3. Document your work (preferably in the assigned wiki space).

Authorship Rules:

Assignments are used both to help you learn about computer concepts and to evaluate your progress (i.e. your grade). In some ways, each assignment is like a take home quiz. Thus, these rules are in effect:

1. You MAY get help from instructors or other students. Such help must be directed toward teaching general concepts, techniques, etc. Post questions in the discussion area if necessary.

2. You may NOT copy another student's work either in whole or in part. Concrete examples are invaluable, but use those in the book and those given in lecture.

3. If in doubt if the help you are giving or receiving is permissible, ask!

4. Since there may be additional questions, I have copied below the entire section from the ICC Student Handbook (2011 – 2012 edition, page 6). I will follow these guidelines in the event of any academic misconduct.

"Matters relating to academic honesty or contrary action such as cheating, plagiarism, or giving unauthorized help on examinations or assignments may result in an instructor giving a student a failing grade for the assignment, test, or course.

Based on the severity of the offense, the instructor may recommend dismissal from the college.

A common form of academic dishonesty is plagiarism. This is the use (whether deliberate or unintentional) of an idea or phrase from another source without proper acknowledgment of that source. The risk of plagiarism can be avoided in written work by clearly indicating, either in footnotes or in the paper itself, the source of any other major or unique idea which the student could not or did not arrive at independently. These precise indications of sources must be given regardless of whether the material is quoted directly or paraphrased. Direct quotations, however brief, must be enclosed in quotation marks as well as being properly documented.

Another form of plagiarism is copying or obtaining information from another student. Submission of written work, such as laboratory reports, computer programs, or papers, which have been

copied from the work of other students, with or without their knowledge and consent, is plagiarism.

Obtaining an examination prior to its administration or use of unauthorized aides during the examination are clear acts of academic dishonesty. It is also academically dishonest to knowingly aid another student in performing an act of academic dishonesty. Thus, in cases of inappropriate collusion on academic work, the provider of inappropriately used material is guilty of academic dishonesty, as well as the actual perpetrator.

Listed below are examples which may involve confusion on the student's part, especially freshmen who are accustomed to working on projects in laboratories with fellow students in high school.

1. Sharing information in the preparation of a report or paper, unless approved by instructor.
2. Turning in the same paper for two different courses with slight modification.
3. The illegitimate uses of written material such as laboratory reports and computer programs or the obtaining of information from other students while an examination is in progress.

In brief, any act which represents work not one's own as one's own is an academically dishonest act. If a student is ever in doubt about an issue of academic dishonesty, or has any hesitation about a contemplated course of action, the student should consult his or her instructors. The penalties for academic dishonesty can be very painful and can affect the entire educational experience at Illinois Central College." (quoted from IC Student Handbook, 2011 – 2012 edition, page 6).

A copy of your student handbook can be found at: **http://markdubois.me/ICCHandbook**

Be Courteous!

1. Cell phones should be silent (off or in vibration mode) – I keep mine that way, why should you be any different…
2. If necessary, take phone calls outside of the class, away from the classroom door
3. Do NOT complete computer labs or surf the Internet or print assignments during lecture/ discussion unless otherwise requested
4. Lab activity tends to generate noise. If you need to read the instructions or take a break, you are welcome to user the areas and facilities surrounding the classroom within reason.