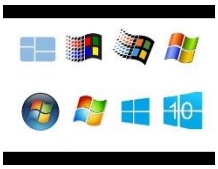
CYB-530 Fall 2018
Securing and Administering Windows Systems

Dates:	Time:	Location:
08/21-12/13/2018	Online	online
Instructor:	**Office Hours:**	**Contact:**
Sonja Streuber	M-F 10-11 am on Google Hangouts	sonja.streuber@valpo.edu

Introduction



Welcome to CYB-530 Securing and Administering Windows Systems! This 3-credit course is an introduction to developing and managing operating system security in a Microsoft Windows environment, specifically Windows 10 and Windows Server 2016. Topics include processes, scheduling, synchronization, memory administration, file system and user account security, PowerShell, and more. The hands-on labs include common operating system utilities and commands, as well as shell programming and network security management within Windows Server.

Learning Objectives

At the end of the course, students will be able to effectively manage and secure computers in a Microsoft Windows personal computer and server environment, specifically to:

1. Evaluate an organization's security computing needs
2. Design the optimal operating system solution
3. Install and configure Windows operating systems for optimal hardware protection
4. Identify, select, and implement an appropriate controls framework to reduce organizational IT risk, incl. hardware and software access and authorization management
5. Perform crucial system administration tasks to “harden” servers and other network equipment
6. Perform forensic tasks to support incident analysis
7. Use Windows shell scripting to automate security mechanisms

Course Format and Attendance Requirement

This is an online course, which means that you will be participating remotely. It does, however, NOT mean that you can log on only once a week. The goal in an online environment is to learn through constant engagement with the material and by communicating with the instructor and your peers. Plan for 9-10 hours worth of work EACH WEEK.

The class rhythm is as follows:

- **Monday**: Do ALL the readings and work through all chapter exercises
- **Tuesday**: Review the weekly lab assignment with your team & determine who does what
- **Wednesday by 11:59 pm CST**: Answer the discussion question, complete work for the lab
- **Thursday**: Review and integrate each team member’s lab contribution into ONE document
- **Friday by 11:59 pm CST**: Respond to TWO of your peers’ posts; upload the team weekly lab
- **Saturday by 11:59 pm CST (or before!)**: Final deadline for the weekly lab assignment

Textbooks & Materials

- In the quickly moving world of MS Windows, books are often outdated as soon as they are published. This is why readings are assigned on a chapter-by-chapter basis from various textbooks, trade publications, and blogs; readings and supplemental slides are posted in the weekly Content folders
- A laptop computer (Windows, Mac, or Linux). You must have administrator permissions.
- Windows 10 Education Edition, Windows 2016 Server, Oracle VirtualBox (if you are choosing to install these OSs as Virtual Machines), available at https://www.virtualbox.org/ .

RECOMMENDED:

- Solomon, Michael G (2014). Security Strategies in Windows Platforms and Applications. Jones&Bartlett. This may be an older book, but it is highly recommended because the concepts discussed are general Windows concepts that will be used in this course.
- Stokes, Jeff, Manuel Singer and Richard Diver (2017). Windows 10 for Enterprise Administrators. Packt Publishing. https://www.amazon.com/Windows-10-Enterprise-Administrators-Redstone/dp/1786462826
- Panek, William (2017). MCSA Windows Server 2016 Study Guide: Exam 70-740. Wiley. Available as free eBook at https://ebookcentral.proquest.com/lib/valpo-ebooks/detail.action?docID=4875027
- Miroshnikov, Andrei (2016). Windows Security Monitoring. Wiley. This book digs deep into Windows auditing, logging, and event systems.
- Gibson, Darril (2011). Microsoft Windows Security Essentials. Wiley. This book is older, but the author is one of the foremost cybersecurity experts in the US. This course references some of the important security concepts from this book. Available as free eBook at https://ebookcentral.proquest.com/lib/valpo-ebooks/detail.action?docID=693645
- Savill, John (2016), Mastering Windows Server Hyper-V. Wiley. Available as free eBook at https://ebookcentral.proquest.com/lib/valpo-ebooks/detail.action?docID=4751489
- Hassell, Jonathan (2017). Learning PowerShell. DEG Press. This book is a quick, but effective, course in itself on learning how to use PowerShell if you aren't too comfortable with programming. Available as free eBook at https://ebookcentral-proquest-com.ezproxy.valpo.edu/lib/valpo-ebooks/detail.action?docID=4947050

Workload and Grading

This 3-credit course requires significant research and teamwork. You will be completing the following:

- **Attendance & Preparation (10 points per week = 150 points total):** Each Wednesday, answer a question in the weekly discussion forum (5 pts). Each Friday, respond to TWO of your peers' responses (5 pts). This activity cannot be made up.
- **Labs (20 points each = 200 points total):** The course contains ten lab assignments about theoretical, practical, or programming problems; depending on enrollment, these may be solved

in standing teams of 2 or 3. Solutions must be posted on Blackboard by 11:59 pm CST on Saturday evening. NO EMAIL SUBMISSIONS WILL BE ACCEPTED.
    - If you are not happy with your grade, you may **revise and resubmit TWO** of the 10 lab assignments. The revisions must follow the comments you have received on the original submissions and present a significant improvement over the original. All revisions MUST be submitted to Blackboard before the end of Week 12 (SAT 11:59 pm CST).
- **Final Lab (50 points):** The final lab will be a comprehensive study of an assigned Windows 10 or Server 2016 incident with technical remediation path. You will present the theoretical portion of the case in a PowerPoint slide deck and demonstrate the technical aspect live. You will use Screen-Cast-O-Matic and your webcam to record your presentation of this PowerPoint and upload the file to YouTube. The YouTube settings must be as follows: Video must be unlisted, Title must include your name, the name of the case, and the name of this semester. Description must show a two-sentence summary of the central issue in your case. **The Take-Home Final is due on Wednesday, December 12, at 12:30 pm CST. No late submissions will be considered.**

You can score a total of 400 points in this course. There will be no extra credit assignments.

Letter Grade Conversion:

>93%: A	90-93%: A-	87-90%: B+	83-87%: B	80-83%: B-	77-80%: C+
73-77%: C	70-73%: C-	<70%: F			

Assignment Submission, Late Work, and Academic Honesty

- **Assignment Submission:** All Assignments must be submitted on Blackboard by 11:59 pm CST on the day they are due (consult the course schedule). No emailed assignments will be accepted.
- **Late Work:** Work is considered late if not posted to Blackboard by 11:59 pm CST on the day it is due (consult the course schedule). Late work will lose 50% of the grade. If work is more than 1 week late, it will receive 1 point only.
- **Academic Honesty:** All work you submit for any course at Valparaiso University—and in any professional environment—must be your own. You may NOT use anyone else's words (from books, blogs, webpages, magazine articles, purchased solutions, etc.) without giving a clear source citation in a footnote. For websites, this includes at a minimum the name of the website, author of the page (if available), date accessed, and URL. You can find the exact APA format at this website: http://www.easybib.com/reference/guide/apa/website

  Please also watch this video about the Valparaiso University Honor Code. If you are still unsure, consult http://www.plagiarism.org/ or the Writing Center.

  In addition, you must write out and sign with your full name the following statement on all deliverables submitted for academic credit:

  I have neither given nor received, nor have I tolerated others' use of unauthorized aid.

  For more information about Valparaiso University's Academic Honor Code, case review cycles, and potential penalties, please refer to http://www.valpo.edu/student/honorcouncil/index.php

Any work found to violate the Valparaiso University Honor Code will receive 0 points and be referred to the appropriate administrative unit.

Diversity and Inclusion

Valparaiso University aspires to create and maintain a welcoming environment built on participation, mutual respect, freedom, faith, competency, positive regard, and inclusion. This course will not tolerate language or behavior that demeans members of our learning community based on age, ethnicity, race, color, religion, sexual orientation, gender identity, biological sex, disabilities (visible and invisible), socio-economic status, or national origin. The success of this class relies on all students' contribution to an anti-discriminatory environment where everyone feels safe, welcome, and encouraged to engage, to explore, and ultimately, "to embark on a rewarding personal and professional journey" (Pres. Heckler).

Title IX

Valparaiso University strives to provide an environment free of discrimination, harassment, and sexual misconduct (sexual harassment, sexual violence, dating violence, domestic violence, and stalking). If you have been the victim of sexual misconduct, we encourage you to report the incident. If you report the incident to a University faculty member or instructor, she or he must notify the University's Title IX Coordinator about the basic facts of the incident. Disclosures to University faculty or instructors of sexual misconduct incidents are not confidential under Title IX. Confidential support services available on campus include: Sexual Assault Awareness & Facilitative Education Office "SAAFE" (219-464-6789), Counseling Center (219-464-5002), University Pastors (219-464-5093), and Student Health Center (219-464-5060). For more information, visit http://www.valpo.edu/titleix/ .

Access and Accommodation Services

The Access & Accommodations Resource Center (AARC) is the campus office that works with students to provide access and accommodations in cases of diagnosed mental or emotional health issues, attentional or learning disabilities, vision or hearing limitations, chronic diseases, or allergies. You can contact the office at aarc@valpo.edu or 219.464.5206. Students who need, or think they may need, accommodations due to a diagnosis, or who think they have a diagnosis, are invited to contact AARC to arrange a confidential discussion with the AARC office. Further, students who are registered with AARC are required to contact their professor(s) if they wish to exercise the accommodations outlined in their letter from the AARC.

Academic Support

To get help, use the Academic Success Center (ASC) online directory (valpo.edu/academicsuccess) or contact the ASC (academic.success@valpo.edu) to help point you in the right direction for academic support resources for this course. Valpo's learning centers offer a variety of programs and services that provide group and individual learning assistance for many subject areas. These learning centers include:

- Graduate Tutoring Lab: Serves the academic needs of Graduate students – tutors offer suggestions on organization of papers, assist in research and citations, and help in understanding difficult assignments. Additional one on one tutoring is also available.
- Writing Center: Primarily serves the needs of undergraduate students, but is also available for Graduate students. Writing Consultants provide proofreading and editing assistance.

Class Cancellations

Notifications of class cancellations will be made through Blackboard with as much advance notice as possible. It will be both posted on Blackboard and sent to your Valpo e-mail address. If you don't check your Valpo e-mail account regularly or have it set-up to be forwarded to your preferred e-mail account, you may not get the message. Please check Blackboard and your Valpo e-mail (or the e-mail address it forwards to) before coming to class.

Work Schedule

Week	Start (2018)	Weekly Topic	Readings (and add'l links on BB), due MON	Due 11:59 pm CST
1	08/21	Introduction	Gibson 1	**W:** Disc. Post **F:** 2 Responses
2	08/26	The Threat Landscape	Gibson 2 Solomon 1	**W:** Disc. Post **F:** 2 Responses **S:** LAB_01
3	09/02	Microsoft Operating System Architecture: Installing Windows 10 and Windows Server 2016 in the Enterprise	Solomon 2 Panek 1,2	**W:** Disc. Post **F:** 2 Responses **S:** LAB_02
4	09/09	Introduction to PowerShell	Hassell 1,2,5,7	**W:** Disc. Post **F:** 2 Responses **S:** LAB_03
5	09/16	Access Controls in MS Windows	Gibson 3, 4 Solomon 3	**W:** Disc. Post **F:** 2 Responses
6	09/23	Group Policy and Active Directory	Solomon 6	**W:** Disc. Post **F:** 2 Responses **S:** LAB_04
7	09/30	Logging and Auditing	Solomon 7 Panek 9	**W:** Disc. Post **F:** 2 Responses
8	10/07	Backup and Recovery	Solomon 8 Panek 3 Savill 7, 8	**W:** Disc. Post **F:** 2 Responses **S:** LAB_05
9	10/14	Network Security	Solomon 9 Panek 5	**W:** Disc. Post **F:** 2 Responses **S:** LAB_06
10	10/21	Encryption	Solomon 4	**W:** Disc. Post **F:** 2 Responses
11	10/28	Hardening the Microsoft Windows Operating System	Solomon 11	**W:** Disc. Post **F:** 2 Responses **S:** LAB_07
12	11/04	Microsoft Application Security	Solomon 12	**W:** Disc. Post **F:** 2 Responses **S:** LAB_08
13	11/11	Virtualization with Hyper-V on Server 2016	Panek 2 Savill 1-4	**W:** Disc. Post **F:** 2 Responses **S:** LAB_09
14	11/25	Microsoft Windows Security Administration	Solomon 10 Panek 8	**W:** Disc. Post **F:** 2 Responses **S:** LAB_10
15	12/02	Developing an Organizational Windows Security Policy	Solomon 15	**W:** Disc. Post **F:** 2 Responses
FINAL	12/12 12:30 pm CST	COURSE FINAL TAKE HOME LAB due on Blackboard		TAKE HOME FINAL DUE

APPENDIX

Student Learning Objectives—Graduate School

1. Students will understand and practice methods of inquiry and strategies of interpretation within the student's field of study.
2. Students will master the knowledge and skills pertinent to the student's field of study.
3. Students will effectively articulate the ideas, concepts, and methods through written and oral presentation.
4. Students will understand the connection between their knowledge and skills on the one hand and their professional identity, responsibilities, and demands on the other.
5. Students will integrate knowledge and methods of their study with cognates and other disciplines.
6. Students will study, reflect upon, and practice ethical behavior and cultural sensitivity as they relate to professional and personal responsibility.

Student Learning Objectives—Information Technology Program (Graduate)

1. To understand and practice methods of inquiry and strategies of interpretation within the student's field of study.
   1A. Students will master several programming environments.
   1B. Students will learn to identify and isolate problems.
2. To master the knowledge and skills pertinent to the student's field of study.
   2A. Students will acquire an extensive technology related vocabulary.
   2B. Students will become comfortable using a wide range of technology environments.
3. To effectively articulate the ideas, concepts, and methods through written and oral presentation.
   3A. Students will be taught how to make formal, oral presentations and be required to give 6 such presentations during their program.
   3B. Students will write numerous, thorough papers requiring extensive research. They will be required to use the services on the writing center.
4. To understand the connection between their knowledge and skills on one hand and their professional identity, responsibilities, and demands on the other.
   4A. Students will understand the implications of legal and professional regulations as they relate to information technology.
   4B. Students will study how technology can be made available to people that are traditionally less advantaged.
5. To integrate knowledge and methods of their study with cognates and other disciplines.
   5A. Students will learn techniques of modeling data from other disciplines.
   5B. Students will study human factors in IT.
6. To practice ethical and cultural sensitivity as it relates to professional and personal responsibility.
   6A. Students will examine a wide range of ethical issues related to technology and the potential effects on people and the environment.
   6B. Students will explore the relationship between IT and ethnic and cultural diversity.

Student Learning Objectives—Computer Science Majors (Undergraduate)

1. Students will demonstrate expertise in the development and design of software.
2. Students will have a working knowledge of the theoretical foundations of the discipline.
3. Students will demonstrate the ability to communicate computer science-related topics in written and oral form.
4. Students will demonstrate that they are informed citizens in the social and ethical implications of the use of computer technology.
5. Students will utilize their computer science education in either their careers or in the pursuit of graduate work.