Student Syllabus
CS 331
Computer Security and Information Assurance
Fall 2016

Instructor: Vince Skinner, CISSP, CISM, CISA, MCSE
Class Meeting Time: 6:00PM-7:15 PM every Monday and Wednesday
Class Location: City Center Plaza Rm 260
Contact Info: vinceskinner@gmail.com, vincentskinner@boisestate.edu
Phone #: 208-830-4492

Course Description:

CS 331 Computer Security and Information Assurance – The course will focus on security goals, access control, common software and network vulnerabilities, cryptography, security policies and procedures.

Course objectives CS 331:

- Information Systems Security
- Security Culture
- Malicious attacks, threats, vulnerabilities
- Access Controls
- Security Operations and Administration
- Auditing, Testing, Monitoring
- Risk, Response, and Recovery
- Cryptography
- Networks
- Malicious Code
- Security Standards
- Security Education
- Security Certifications
- May have more or less topics based on the available lectures

Prerequisites:

CS 252 or CS 253, or ITM 225 and ITM 305.

Student Textbook

Primary Text
Fundamentals Of Information Systems Security
ISBN-13: 978-1284031621
ISBN-10: 1284031624

Instructor Notes:

- Be prepared for lab and class. (paper, pen, book, etc)
- If you miss a class, get the homework from a classmate or instructor.
- 80% of life (school) is showing up.
- The Midterm & Final Exams will be based upon quizzes, in-class discussion, textbook reading, textbook questions and other materials.
- **Late Work Policy**: Late work will be accepted but with severe penalties, unless prior notification is given prior to absence.
  - The ultimate success of a student depends upon his/her timely completion of course work as well as the resulting feedback.
  - Students are responsible for their course work.

  - Course work turned in late detracts from the learning environment because every class session builds upon a previous session.
  - Course work not completed on time impacts student preparation for the next set of objectives.
- Create Backup copies of your homework.
- Send homework to your instructor via email in this format "Class.Week.Lab/homework.doc"
  - Example – CS331.week1.lab.doc or CS331.week1.homework.doc
- No excuses, I'm training you for the workplace.
- First Assignment is to send the instructor an email stating:
  - Subject: BSU Student Info - <Student Name>
  - Your Name:
  - Class Number/Name
  - Email Address:
  - Acknowledgment and Understanding of this Syllabus
  - My Primary phone# is:

Category Weights:

Final Grades will be calculated from the percentages earned in class as follows:

Participation	**10%**
Homework Assignments	**10%**
Labs	**25%**
Project–Top 5 Technologies	**15%**
Project–Top 5 Skills/Processes	**15%**
Final Exam	**25%**

A	90-100%	4.0
B+	85-89%	3.5
B	80-84%	3.0
C+	75-79%	2.5
C	70-74%	2.0
D+	65-69%	1.5
D	60-64%	1.0
F	<59%	0.0

No.	Date	Read / Topic – This schedule is subject to change.
1	8/22 8/24	**Computer Security and Information Assurance** **Read Chapter 1 – Information Systems Security** **Research Assignment** – Technical Research Paper on the current technologies and processes that companies are utilizing to secure their infrastructures. **Lab** – Implement an enterprise log mgmt solution to collect logs for lab work through out the semester. **Semester Project Overviews** Top 5 Protective Technologies and Processes - Develop a technology configuration that a security professional would implement to maximize the most security with the least amount of effort. Top 5 Offensive Technologies and Processes – Develop a technology configuration that a security professional would implement to maximize the most amount of impact on an organization.
2	8/29 8/31	**Research Assignment** – Technical Research Paper on the most utilized and affective attacks used today. How can organizations make their systems more secure when considering these new attacks. **Lab** – Begin to feed your log mgmt solution with some logs.
3	9/5 9/7	Labor Day – NO CLASS **– September 7th and 9th.** **Read Chapter 2 – Changing how people and business communicate** **Research Assignment** – Technical Research Paper on how telephones and telephony technologies are utilized today to conduct attacks on organizations. **Lab** – Continue to become more familiar with the log mgmt solution and the ability to search.
4	9/12 9/14	**Read Chapter 3 – Malicious attacks, threats, vulnerabilities** **Research Assignment** – Technical Research Paper on the top 5 most affective attacks on organizations today and what threats/vulnerabilities were part of the attacks. **Lab** – Utilizing the provided samples, observe the methods utilized by the malicious code.
5	9/19 9/21	**Read Chapter 4 - Drivers of the information security business** **Research Assignment** – Technical paper on the discovery and recovery mechanisms when a breach or ransomeware infection is present. **Lab** – Create a repeatable process and technical tests by which the security results can be distilled and show actual risks to an organization.

6	9/26 9/28	**Read Chapter 5 - Access Controls** **Research Assignment** – Technical Research Paper on the various types of access control methods; which are most affective, easiest to manage and where(Technologies) would you want to deploy them. **Lab** – Create a process on your windows domain to allow others to connect to a share, capture the login information(User, Times, etc), and identify what the user touched on the file server. Limit access times to only certain times. For extra credit, setup RDP access utilizing DUO.
7	10/3 10/5	**Read Chapter 6 - Security Operations and Administration** **Research Assignment** – Write a technical research paper on the incident response plan that you would create . **Lab –** Create a technical implemented solution to monitor and control changes(Applications installed and those that run in Appdata) on your desktops and servers.
8	10/10 10/12	**Read Chapter 7 - Auditing, Testing and Monitoring** **Research Assignment** – Write a technical research paper on what tests every company should conduct on their network and endpoints and the controls to implement to remediate the results of the tests. **Lab** – Utilize tools to test egress filtering on firewalls/proxy. Utilize tools to test the ability to install backdoors on an endpoint.
9	10/17 10/19	**Read Chapter 8 – Risk, Response, and Recovery** **Research Assignment** – Write a technical research paper on the methodology that would be utilized to show actual risks of an organization and how they would recover from those risks. **Lab** – Install and configure a solution to recover from a ransomware attack.
10	10/24 10/26	**Read Chapter 9 – Cryptography** **Research Assignment** – Write a technical research paper where the application of cryptography can help reduce risk on an organization. **Lab** – 1 - Design and implement an implementation of cryptography to protect files on a file server that are used by various users. 2 – Send an encrypted email and attachment utilizing asymmetric and symmetric encryption.
11	10/31 11/2	**Read Chapter 10 – Networks and telecommunications** **Research Assignment** – Write a technical research paper on the requirements of a firewall and the advantages and disadvantages that firewalls have to reduce risk to an organization. **Lab** – Install and configure a firewall; configuring by least privilege; allowing internal clients to get to certain websites and allowing external access to a webserver.

12	11/7 11/9	**Read Chapter 11 – Malicious Code and Activity** **Research Assignment** – Write a technical research paper on the method of deployment of the top 5 malicious code samples and how they can be remediated. **Lab** – Deploy two methods of detecting an infection of malicious code.
13	11/14 11/16	**Read Chapter 12 – Information Security Standards** – Write a technical research paper on the methodology you would use deploy a standard to server, desktops, and laptops. **Lab** – Install and configure a baseline group policy to minimize infection.
14	11/21 11/23	Thanksgiving – No Class
15	11/28 11/30	**Read Chapter 13 – Education and Training** **Research Assignment** – Write a technical research paper on the best methodology to educate end users; think about the technicial methods you would use to teach them about today's risks. **Lab** – Configure a technical process/technology to alert users when unapproved applications are installed; even in appdata.
16	12/5 12/7	**Read Chapter 14/15 – Professional Certification & US Compliance Laws** – Write a research paper on which technical certifications are the best to obtain and why. **Lab** – We will review your solutions for the semester projects
17	12/12	Final Exam

Notice of Policy on Scholastic Dishonesty

The following statement is the university's policy on academic honesty. It applies to conduct in this class:

> The university's goal is to foster an intellectual atmosphere that produces educated, literate people. Because cheating and plagiarism are at odds with that goal, they shall not be tolerated in any form. Students are expected to adhere to the rules and regulations as set forth in the Student Code of Conduct. Therefore, all work submitted by a student must represent that student's own ideas and effort; when the work does not, the student has engaged in academic dishonesty.
>
> Plagiarism occurs when a person passes in another person's work as his or her own or borrows directly from another person's work without proper documentation. For example, academic dishonesty occurs whenever a student:
>
> - Buys a paper or other project, then seeks to receive credit for the paper or project
> - Copies from another student's exam, either before, during, or after the exam
> - Uses "crib notes" while taking an exam or uses information stored in a computer or calculator (if prohibited from doing so)
> - Allows another person to take an exam in his or her place or takes an exam for another person
> - Collaborates on take-home exams when such collaboration is forbidden
> - Copies the work of another person and attempts to receive credit for that work
> - Fails to properly document source material in a paper or project
> - Receives editorial assistance that falls outside the scope of acceptable assistance
>
> NOTE: The list above is intended only to provide general guidelines for recognizing and avoiding common types of academic dishonesty. It is in no way an exhaustive or comprehensive list of all the types of academic dishonesty.
>
> Except in cases of major offenses, responding to academic dishonesty is the responsibility of the instructor of the course in which the dishonesty occurs. If a student is responsible of academic dishonesty, the student may be dismissed from the class and may receive a failing grade. Other penalties may include suspension or expulsion from school.

Incidents involving academic dishonesty will be addressed on an individual basis and forwarded with documentation to the appropriate administrative office within the parameters provided through Boise State policy and procedures. Please note that this means a student must clearly distinguish between content that represents their own thought/analysis and written material that is drawn, either completely or paraphrased, from the work of another.