University of Montana
ScholarWorks at University of Montana

Syllabi | Course Syllabi

Fall 9-1-2018

ITS 222.50: Enterprise Security

Zachary L. Rossmiller
University of Montana - Missoula, zachary.rossmiller@umontana.edu

Let us know how access to this document benefits you.

Follow this and additional works at: https://scholarworks.umt.edu/syllabi

Recommended Citation
Rossmiller, Zachary L., "ITS 222.50: Enterprise Security" (2018). *Syllabi*. 8417.
https://scholarworks.umt.edu/syllabi/8417

This Syllabus is brought to you for free and open access by the Course Syllabi at ScholarWorks at University of Montana. It has been accepted for inclusion in Syllabi by an authorized administrator of ScholarWorks at University of Montana. For more information, please contact scholarworks@mso.umt.edu.

MISSOULA COLLEGE
UNIVERSITY OF MONTANA

ITS 222
Enterprise Security
Autumn 2018

Professor Information

Professor:	Zachary L. Rossmiller, MBA (MCSE, MCSA, MS, MCP, Security+, A+, Net+, ITIL v3)
E-Mail:	zachary.rossmiller@umontana.edu
Zoom Room:	https://umontana.zoom.us/my/rossmillerz
Office Hours:	Available by appointment and Zoom

Course Information

Meeting:	Online (WWW)
Section:	01
Credits:	3
Grading Mode:	Traditional letter grade
CRN:	74099
Pre-requisites:	ITS 210 – Network OS – Desktop, ITS 212 – Network OS – Server Administration

Course Description

This course explores general information technology security concepts that will help prepare the student for IT Security in their future career. Topics include: access control, authentication, attack methods, remote access, web security, wireless networks, cryptography, internal infrastructure security, and external attacks. In addition, students will learn industry security procedures, organizational policies, risk management and disaster recovery planning, and risk assessment. Students will use various learning tools, hands on projects and case projects to allow students to implement the practices they will be learning.

Course Learning Objectives

Upon completion of this course, students will be able to:

- Identify potential risks to your network, such as access and denial of service attacks; modification and repudiation attacks; malicious software attacks; and social engineering.
- Understand common remote access options and components, including virtual private networks; and tunneling and point to point protocols.
- Describe network and host-based intrusion detection mechanisms and vulnerabilities.
- Explain the concept of hardening in relation to the OS, hardware, and applications.
- Define the core components of physical network security and the importance of corporate security policies.
- Understand the basic premise of cryptography and public key infrastructure.
- Develop a comprehensive disaster recovery plan for a small business.
- Develop a comprehensive network security plan for a small business.
- Describe and explain the importance of security, ethics, and, privacy issues

Course Overview

ITS 222 Enterprise Security consists of three learning units. The first unit we will cover hardware and communications. Topics will include understanding devices and infrastructure, such as infrastructure terminology, firewalls, VPNs, intrusion detection systems, and load balancers. We will also explore the different types of vulnerabilities, hacktivists, and other issues in IT Security. The second unit will cover software protections and exposures. This will unit will involve using protocol analyzers, network scanners, password

crackers, and vulnerability scanners. Further, we will explore IT security in the "Cloud" and the different terminologies that is often associated with the cloud, such as private versus public cloud, SaaS versus PaaS versus IaaS. Lastly, unit three will cover risk assessment, policy, and business continuity. Topics will include measuring and weighing risk, security administration best practices, disaster recovery planning and incident response. Lastly, unit three will cover how to monitor and diagnose networks using industry best practices.

ITS 222 Enterprise Security is designed so that you understand the critical components of network security. We will cover physical security and devices as well as software and organizational components. By the end of the course you will know the appropriate strategies to implement to prevent security breaches, and you will demonstrate this knowledge by designing a comprehensive network security plan.

This class stems from the CompTIA Security+ (SY0-501) industry certification. Although not all objectives will be covered in this course, a solid foundation will be created to help encourage students to understand Linux server administration. Students with at least a B average in the course will have the option to purchase discounted examination vouchers through the department.

Required Course Materials

CompTIA Security+ Study Guide: Exam SY0-501, 7th Edition, Emmett Dulaney, Chuck Easttom, ISBN: 978-1-119-41689-0

Practice-Labs.com - Security+ SY0-501 Hands-On Labs

A note about the textbook: Make sure to get the seventh edition of the text (released in October 2017), which references the CompTIA Security+ SY0-501 on the cover. The seventh edition is a complete re-write of the book for the new Security+ certification. You cannot use earlier editions of this book.

Grading Course Activities

Moodle will be used to post grades.

Activity	Weight
Course Exams	
Exam 1	
Exam 2	
Exam 3	
Final Exam	
Exam Subtotal	**30%**
Discussion Forums	**10%**
Homework Assignments	**30%**
Labs and Research Assignments	**30%**
Total	**100%**

Grading Scale:	Letter Grade:
100 – 93.00%	A
92.99% - 90.00%	A-
89.99% - 87.00%	B+
86.99% - 83.00%	B
82.99% - 80.00%	B-
79.99% - 77.00%	C+
76.99% - 73.00%	C
72.99% - 70.00%	C-
69.99% - 67.00%	D+
66.99% - 60.00%	D
59.00% - 0.00%	F

***This will be based on time remaining in the semester. Announcements will be made in class. Always check Moodle for the latest version!**

Exams (30%)

There will be three (3) exams throughout the semester (not including the Final Exam). The exams will cover material from the labs, lectures, readings, and textbooks. Each exam will consist of multiple choice, essay questions, and short answer questions. Each exam is worth 100 points. Number of questions will vary per exam.

Final Exam

The final exam is comprehensive and will be given in two parts – a multiple choice exam and a written exam. More information will be made available as we make our way towards the end of the semester.

Online Participation (10%)

In each unit, there will often be a discussion topic. For full credit, I would like you to make an initial post to the forum, answering the question or discussing the issue I've presented. After everyone has made an initial post, you'll respond to the posts of two of your classmates, either asking questions or commenting on their information. The point of the forum is for you to exchange ideas and information with your fellow students. Please post in a positive, contributory manner

Homework and Written Assignments (30%)

As we cover each chapter in the textbook I will assign review questions over the material. These will be assigned as we work through each chapter. In addition to questions in the textbook, I will assign homework that will be relevant to what we are learning during that particular week. I expect them to be typed with proper formatting.

Hands-On Labs and Research Assignments (30%)

As we cover each chapter in the textbook I will assign several online hands-on labs through Practice Labs. In addition, research projects will be relevant to what we are learning during that particular day or week. Research projects could take form in either a formal written document or a PowerPoint presentation. Various research projects could cover security audits, purchase proposal and justification, or educational awareness training for staff. I expect these research projects to be presented as if you were presenting this to your employer, managers, or even Board of Directors. All research projects are to be submitted via Moodle.

Classroom Behavior Expectations

Email

According to University policy, faculty may only communicate with students regarding academic issues via official UM email accounts. Accordingly, students must use their UM accounts. Email from non-UM accounts will likely be flagged as spam and deleted without further response. To avoid violating the Family Educational Rights and Privacy Act, confidential information (including grades and course performance) will not be discussed via phone or email. All email communications should be professional in tone and content. A professional email includes a proper salutation, grammar, spelling, punctuation, capitalization, and signature. Please check your UM email daily so you won't miss important class and COB announcements.

Exam Conduct

Students must take exams on their regularly scheduled days unless they have an excused absence. Excused absences ONLY include (1) University-approved absences, (2) documented health emergencies, (3) civil service such as military duty and jury duty, and (4) other emergencies deemed appropriate by the instructor. In all cases, the instructor must be notified prior to the exam unless the emergency makes such notification infeasible. During the exam, you may not leave the room for any reason. Doing so results in the conclusion of that student's exam. Electronic dictionaries, cell phones, tablets, laptops, notes, smart watches, or other assistive items are not allowed.

Academic Misconduct

All students must practice academic honesty. Academic misconduct is subject to an academic penalty by the course instructor and/or a disciplinary sanction by the University. The University of Montana Student Conduct Code specifies definitions and adjudication processes for academic misconduct and states, "Students at the University of Montana are expected to practice academic honesty at all times." IMPORTANT: It is the student's responsibility to be familiar with the Student Conduct Code, including definitions of academic misconduct. (found online at http://www.umt.edu/vpsa/policies/student_conduct.php).

Using the Web to research materials and concepts is an integral part of learning in the twenty-first century. Studying with other students is a productive method of learning. A certain amount of collaborating on concepts with other students and using resources found on the Internet in an assignment is recommended. Copy and paste is not acceptable. It is expected that each student will input his/her assignment into the computer, and each student must be able to explain any assignment turned in. Collaboration on exams is strictly forbidden.

Student Resources

Writing Center

For students who wish to improve their written communication skills, the Writing Center offers free, one-on-one tutoring to undergraduate and graduate students in all disciplines. The center provides "a comfortable environment where students can engage in supportive conversations about their writing and receive feedback on their works in progress. Our professional tutors help students at any point during a writing process and with any writing task." For additional information, please visit the Writing Center's website at http://www.umt.edu/writingcenter.

Disability Services for Students

Students with disabilities will receive reasonable modifications in this course. The student's responsibilities are to request them from me with sufficient advance notice and to be prepared to provide official verification of disability and its impact from Disability Services for Students. Please speak with me after class or during my office hours to discuss the details. For more information, visit the website for the office of Disability Services for Students (found online at http://www.umt.edu/dss/).

Course Schedule

Since the course schedule is tentative and subject to change throughout the semester, it has been posted as a separate document on Moodle. The course schedule can be located on Moodle under *Course Schedule*. Please refer to the course schedule on a weekly basis to stay abreast of upcoming course events, lecture materials, and assigned readings.

Syllabus Revision

Instructor reserves the right to modify syllabi and assignments as needed based on faculty, student, and/or environmental circumstances. If changes are made to the syllabus, amended copies will be dated and made available to the class through Moodle.

Last Revised: August 26, 2018

Topic Outline

1. Unit 1 – Hardware and Communications
    1. Chapter 3 – Understanding Devices and Infrastructures
    2. Chapter 7 – Host, Data, and Application Security
    3. Chapter 5 – Wireless Network Threats

2. Unit 2 – Software Protections and Exposures
    1. Chapter 4 – Identity and Access Management
    2. Chapter 6 – Securing the Cloud
    3. Chapter 9 – Threats, Attacks, and Vulnerabilities
    4. Chapter 8 – Cryptography
    5. Chapter 10 – Social Engineering and Other Foes

3. Unit 3 – Risk Assessment, Policy, and Business Continuity
    1. Chapter 1 – Managing Risk
    2. Chapter 11 – Security Administration
    3. Chapter 12 – Disaster Recovery and Incident Response
    4. Chapter 2 – Monitoring and Diagnosing Networks