ISSC242

Course Summary

Course : ISSC242 **Title :** Hardening Operating Systems **Length of Course :** 8 **Faculty :** **Prerequisites :** N/A **Credit Hours :** 3

Description

Course Description:

This course is a study of the principles and concepts of Network Security from the perspective of the
Operating System (OS). It places emphasis on discovering the vulnerabilities of the standard Operating Systems (OS) to attacks and focuses on the methodologies and measures necessary to take a proactive and preventive stance to address security vulnerabilities. Students will examine the principles, practices, and policies related to hardening and securing Operating Systems so they are impervious to security threats. It focuses on the vulnerabilities and the related countermeasures of various Windows components (Domain structures, domain trusts, security account manager, policies, profiles, file system, IP services (DHCP, DNS, IIS, TCP/IP printing, RPC, RIP for Internet protocol, SNMP), DCOM, Registry, Active Directory, Encrypting File System (EFS), IPSec, and public key certificate services). This course also discusses vulnerabilities and countermeasures related to UNIX (file This course is a study of the principles and concepts of Network Security from various aspects including but not limited to hardware, software, operation systems, and other critical elements relating to the CIA Triad. There is an emphasis on standard Operating System (OS) functions and discovering associated vulnerabilities. Upon completion of this course, students will be able to demonstrate an understating of methodologies and measures necessary to take a proactive and preventive stance to address security vulnerabilities. Students will examine the principles, practices, and policies related to hardening and securing Operating Systems so they are impervious to security threats. It focuses on the vulnerabilities and the related countermeasures of various Windows components (Domain structures, domain trusts, security account manager, policies, profiles, file system, IP services (DHCP, DNS, IIS, TCP/IP printing, RPC, RIP for Internet protocol, SNMP), DCOM, Registry, Active Directory, Encrypting File System (EFS), IPSec, and public key certificate services).

Course Scope:

This course focuses on new risks, threats, and vulnerabilities associated with the Microsoft Windows operating system. It also emphasizes how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. Lastly, it is a resource for students desiring more information on Microsoft Windows OS hardening, application security, and incident management, among other issues.

Objectives

The successful student will fulfill the following learning objectives:

1. List key concepts and terms associated with information systems security
2. Identify risks, threats, and vulnerabilities associated with the Windows operating systems
3. Align security procedures and practices with protecting Windows systems
4. Manage security incidents involving Windows operating systems and applications
5. Design security controls to keep Windows computers secure
6. Configure Windows controls to protect both server and client computers

Outline

Week 1:

Topic(s)

Textbook:

Chapter 1: Microsoft Windows in the Landscape

Chapter 2: Security in the Microsoft Windows Operating System

Learning Objective(s)

CO1:List key concepts and terms associated with information systems security

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

Assignment(s)

Discussion #1

Week 1 Assignment

Lab #1

Week 2:

Topic(s)

Textbook:

Chapter 3:Access Control in Microsoft Windows

Chapter 4:Microsoft Windows Encryption Tools and Technologies

Learning Objective(s)

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

CO3:Align security procedures and practices with protecting Windows systems

Assignment(s)

Discussion #2

Lab #2

Week 3:

Topic(s)

Textbook:

Chapter 5: Protecting Microsoft Windows Against Malware

Chapter 6: Group Policy Control in Microsoft Windows

Chapter 7: Microsoft Security Profile and Audit Tools

Learning Objective(s)

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

CO3:Align security procedures and practices with protecting Windows systems

Assignment(s)

Discussion #3

Lab #3

Week 4:

Topic(s)

Textbook:

Chapter 8:Microsoft Windows Backup and Recovery Tools

Learning Objective(s)

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

CO5:Design security controls to keep Windows computers secure

Assignment(s)

Discussion #4

Lab #4

Week 5:

Topic(s)

Textbook:

Chapter 9: Microsoft Windows Network Security

Chapter 10:Microsoft Windows Security Administration

Chapter 11: Hardening the Microsoft Windows Operating System

Learning Objective(s)

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

CO6:Configure Windows controls to protect both server and client computers

Assignment(s)

Discussion #5

Lab #5

Week 6:

Topic(s)

Textbook:

Chapter 12: Microsoft Application Security

Chapter 13: Microsoft Windows Incident Handling and Management

Learning Objective(s)

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

CO4:Manage security incidents involving Windows operating systems and applications

Assignment(s)

Discussion #6

Lab #6

Week 7:

Topic(s)

Textbook:

Chapter 14:Microsoft Windows and the Security Life Cycle

Chapter 15: Best Practices for Microsoft Windows and Application Security

Learning Objective(s)

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

CO3:Align security procedures and practices with protecting Windows systems

Assignment(s)

Discussion #7

Lab #7

Week 8:

Topic(s)

Textbook:

No Readings Assigned

Learning Objective(s)

CO2:Identify risks, threats, and vulnerabilities associated with the Windows operating systems

CO5:Design security controls to keep Windows computers secure

Assignment(s)

Discussion #8

Lab #8

Project Paper

Evaluation

The grading will be based on five graded Weekly assignments, eight weekly Discussion postings, and an individual project

1. There will be eight weekly Discussion postings you will need to respond to. Answers should **restates the question** and **support** your position using the terms, concepts, and theories from the required readings. You may **attack**, **support** or **supplement** other students' answers using the terms, concepts and theories from the required readings. You may respond multiple times with a continuous discussion with points and counter points. The key requirement is to express your idea and then **support your position** using the terms, concepts and theories from the required readings to demonstrate to me that you understand the material. The Discussion postings will count as 30%. All discussion posts must be original work. For full credit consideration, you

must post your initial posting by Wednesday and respond to a minimum of two peers with value added feedback.

1. There will be 1 short essay assignment counting a total of 10% of the final grade. The reviews will follow each of the major milestones of the course. These reviews will be recaps of the week's Week. They are selected to provide the student with an opportunity to state what they have learned from the Week and to verify they have a grasp of the material.

- There will be eight labs which will count 30% of the final grade. The format for the lab report is listed under the assignment for lab reports.
- :

1. The Project Paper will count as 30% of the final grade and is due the end of week 8. The requirements for the project paper are listed under the assignment for the project paper.

Grading:

Name	Grade %
Discussions	30.00 %
Discussion #1	
Discussion #2	
Discussion #3	
Discussion #4	
Discussion #5	
Discussion #6	
Discussion #7	
Discussion #8	
Assignments	10.00 %
Week 1 Assignment	10.00%
Labs	30.00 %
Lab #1	
Lab #2	
Lab #3	
Lab #4	
Lab #5	
Lab #6	
Lab #7	
Lab #8	

Week 8 Project Paper	30.00 %

Materials

Book Title: Security Strategies In Windows Platforms And Applications, 3rd ed - the e-book is provided inside the classroom

Author: Solomon

Publication Info: VS-Jones & Bartlett

ISBN: 9781284175622

Book Title: ISSC342 virtual lab manual provided inside the classroom

Author:

Publication Info: CLASS-Jones & Bartlett

ISBN: 9781284064155

Book Title: Requires CITRIX CLIENT SOFTWARE INSTALLATION FOR ONLINE VIRTUAL LABS accessibility - instructions provided inside the classroom.

Author: No Author Specified **Publication Info: ISBN:** N/A

Required Lab Manual

vLab Solutions (2013). Laboratory Manual Version 1.5 To Accompany Security Strategies In Windows Platforms And Applications. Jones & Bartlett Learning: Information Systems Security & Assurance Curriculum. ISBN: 128403755X 978-1284037555

Instructions to obtain the ebook located in Resources.

Software Requirements to complete Activities and Week Reviews

1. Microsoft Office (MS Word, MS Excel, MS PowerPoint) or comparable document processing format(Mac, Linux, etc.)
2. Adobe Acrobat Reader or comparable pdf viewer
3. Drawing software such as Visio

Course Guidelines

Citation and Reference Style

- Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the APA Format.

Tutoring

- Tutor.com offers online homework help and learning resources by connecting students to certified tutors for one-on-one help. AMU and APU students are eligible for 10 free hours* of tutoring provided by APUS. Tutors are available 24/7 unless otherwise noted. Tutor.com also has a SkillCenter Resource Library offering educational resources, worksheets, videos, websites and career help. Accessing these resources does not count against tutoring hours and is also available 24/7. Please visit the APUS Library and search for 'Tutor' to create an account.

Late Assignments

- Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. The due date for each assignment is listed under each Assignment.
- Generally speaking, late work may result in a deduction up to 10% of the grade for each day late, not to exceed a 50% penalty after 5 days or later.
- As a working adult I know your time is limited and often out of your control. Faculty may be more flexible if they know ahead of time of any potential late assignments.

Turn It In

- Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. This is automatically processed through the Assignments area of the course.

Academic Dishonesty

- Academic Dishonesty incorporates more than plagiarism, which is using the work of others without citation. Academic dishonesty includes any use of content purchased or retrieved from web services such as CourseHero.com. Additionally, allowing your work to be placed on such web services is academic dishonesty, as it is enabling the dishonesty of others. The copy and pasting of content from any web page, without citation as a direct quote, is academic dishonesty. When in doubt, do not copy/paste, and always cite.

Submission Guidelines

- Some assignments may have very specific requirements for formatting (such as font, margins, etc) and submission file type (such as .docx, .pdf, etc) See the assignment instructions for details. In general, standard file types such as those associated with Microsoft Office are preferred, unless otherwise specified.

Disclaimer Statement

- Course content may vary from the outline to meet the needs of this particular group.

Communicating on the Discussion

- Discussions are the heart of the interaction in this course. The more engaged and lively the exchanges, the more interesting and fun the course will be. Only substantive comments will receive credit. Although there is a final posting time after which the instructor will grade comments, it is not sufficient to wait until the last day to contribute your comments/questions on the discussion. The purpose of the discussions is to actively participate in an on-going discussion about the assigned content.
- "Substantive" means comments that contribute something new and hopefully important to the discussion. Thus a message that simply says "I agree" is not substantive. A substantive comment contributes a new idea or perspective, a good follow-up question to a point made, offers a response to a question, provides an example or illustration of a key point, points out an inconsistency in an argument, etc.
- As a class, if we run into conflicting view points, we must respect each individual's own opinion. Hateful and hurtful comments towards other individuals, students, groups, peoples, and/or societies will not be tolerated.

Identity Verification & Live Proctoring

- Faculty may require students to provide proof of identity when submitting assignments or completing assessments in this course. Verification may be in the form of a photograph and/or video of the student's face together with a valid photo ID, depending on the assignment format.
- Faculty may require live proctoring when completing assessments in this course. Proctoring may include identity verification and continuous monitoring of the student by webcam and microphone during testing.

University Policies

Student Handbook

- Drop/Withdrawal policy
- Extension Requests
- Academic Probation
- Appeals
- Disability Accommodations

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.