Preview: IT4080 : Operating Systems and Application Security

Syllabus

Course Overview

This course addresses securing operating systems and applications by identifying areas of vulnerability and the technologies that are available to mitigate those vulnerabilities. The course covers all classes of applications including mobile, E-mail, databases, and Web applications.

Technology Resources

This Capella course offers labs through Jones and Bartlett Learning. These labs offer guided practice in performing tasks related to achieving course competencies and completing assessments. If you require the use of assistive technology or alternative communication methods to participate in these activities, please contact Disability Services to request accommodations.

Course Competencies

(Read Only)

To successfully complete this course, you will be expected to:

1. Describe the various forms of operating systems that are components of a modern network.
2. Identify threats and vulnerabilities specific to operating systems and applications.
3. Describe controls that mitigate operating system and application threats and vulnerabilities.
4. Analyze the various forms of encryption that are used in operating system and application security.
5. Apply mitigations that support operating system and application security within a specific organization.
6. Communicate effectively.

Course Prerequisites

Prerequisite(s): IT4803.

Syllabus >> Course Materials

Required

The materials listed below are required to complete the learning activities in this course.

Integrated Materials

Many of your required books are available via the VitalSource Bookshelf link in the courseroom, located in your Course Tools. Registered learners in a Resource Kit program can access these materials using the courseroom link on the Friday before the course start date. Some materials are available only in hard-copy format or by using an access code. For these materials, you will receive an email with further instructions for access. Visit the Course Materials page on Campus for more information.

eBook

Capella University. (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning. ISBN: 9781284011593.

Library

The following required readings are provided in the Capella University Library or linked directly in this course. To find specific readings by journal or book title, use Journal and Book Locator. Refer to the Journal and Book Locator library guide to learn how to use this tool.

- Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (2nd ed.). Boston, MA: Elsevier Science.
- Calerdon Pale, P. (2012). *Nmap 6: Network exploration and security auditing cookbook.* Birmingham, AL: Packt Publishing.
- Carpenter, T. (2012). *Microsoft Windows operating system essentials.* Hoboken, NJ: Sybex.
- Dulaney, E. A. (2011). *CompTIA security+ study guide: Exam SY0-301* (5th ed.). Indianapolis, IN: Sybex.
- Gibson, D. (2011). *Microsoft Windows security: Essentials.* Indianapolis, IN: Wiley Publishing.
- Hingarh, V., & Ahmed, A. (2013). *Understanding and conducting information systems auditing.* Singapore: Wiley.

- Hoffstein, J., Pipher, J. C., & Silverman, J. H. (2008). *An introduction to mathematical cryptography.* New York, NY: Springer.
- Johnson, S. (2010). *Mastering Microsoft Windows Small Business Server 2008.* Indianapolis, IN: Wiley.
- Konheim, A. G. (2010). *Hashing in computer science: Fifty years of slicing and dicing.* Hoboken, NJ: Wiley.
- Mansfield-Devine, S. (2010). Security through isolation. *Computer Fraud & Security, 2010*(5), 8–11.
- Nahari, H., & Krutz, R. L. (2011). *Web commerce security: Design and development.* Indianapolis, IN: Wiley.
- Ottenheimer, D., & Wallace, M. (2012). *Securing the virtual environment: How to defend the enterprise against attack.* Indianapolis, IN: Wiley.
- Panek, W. (2011). *Microsoft Windows 7 administration instant reference.* Indianapolis, IN: Wiley.
- Skillsoft. (n.d.). *Cloud computing fundamentals: Virtualization and data centers* [Tutorial].
- Skillsoft. (n.d.). *CompTIA CASP CAS-002: Application vulnerabilities and security controls* [Tutorial].
- Skillsoft. (n.d.). CompTIA CASP CAS-002: System, Audit, and Review Logs [Video].
- Skillsoft. (n.d.). *CompTIA CASP CAS-003: Integrating cloud and virtualization technologies in the enterprise* [Tutorial].
- Skillsoft. (n.d.). *CompTIA Security+ 2011: Securing applications, virtualization, and cloud computing* [Tutorial].
- Skillsoft. (n.d.). CSSLP: Database Security [Video].
- Skillsoft. (n.d.). CSSLP: Logging and Auditing [Video].
- Skillsoft. (n.d.). *Microsoft security fundamentals: Operating system security* [Tutorial].
- Skillsoft. (n.d.). Security+: Database Security [Video].
- Skillsoft. (n.d.). Security+: Operating System Security Considerations [Video]
- Smith, R. W. (2012). *Linux essentials.* Indianapolis, IN: Sybex Inc.
- Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information systems security professional study guide* (6th ed.). Indianapolis, IN: Wiley.
- Stuttard, D., & Pinto, M. (2011). The web application hacker's handbook: Finding and exploiting security flaws (2nd ed.). Indianapolis, IN: Wiley.
- Taylor, A. G. (2013). *SQL for dummies.* Hoboken, NJ: Wiley. ISBN: 9781118657188.
- Zalewski, M. (2012). *The tangled web: A guide to securing modern web applications.* San Francisco, CA: No Starch Press.

External Resource

Please note that URLs change frequently. While the URLs were current when this course was designed, some may no longer be valid. If you cannot access a specific link, contact your instructor for an alternative URL. Permissions for the following links have been either granted or deemed appropriate for educational use at the time of course publication.

- CernerEng. (2014). *Application security – Understanding, exploiting, and defending against top Web vulnerabilities* [Video]. Retrieved from http://www.youtube.com/watch?v=sY7pUJU8a7U
- CUFP 2013. (2013). CUFP 2013: Tom Hawkins: Redesigning the computer for security [Video]. Commercial Users of Functional Programming (CUFP), Retrieved from http://cufp.org/2013/tom-hawkins-bae-systems-redesigning-computer-secur.html.

- Microsoft TechEd North America. (2012). The evolution of active directory recovery [Video]. | Transcript Retrieved from https://channel9.msdn.com/Events/TechEd/NorthAmerica/2012/SIA319
- Tuli, P., & Sahu, P. (2013). System monitoring and security using keylogger [PDF]. *International Journal of Computer Science and Mobile Computing, 2*(3), 106–111. Retrieved from http://www.ijcsmc.com/docs/papers/March2013/V2I3201322.pdf
- USENIX Association. (2012). Ask WINE: Are we safer today? Evaluating operating system security [Video]. (31 minutes.) Retrieved from https://www.usenix.org/conference/leet12/workshop-program/presentation/dumitras
- w3resource (2018). NoSQL Introduction. Retrieved September 7, 2018, from https://www.w3resource.com/mongodb/nosql.php

Suggested

The following materials are recommended to provide you with a better understanding of the topics in this course. These materials are not required to complete the course, but they are aligned to course activities and assessments and are highly recommended for your use.

Optional

The following optional materials are offered to provide you with a better understanding of the topics in this course. These materials are not required to complete the course.

Unit 1 >> Operating System Security Basics

Introduction

Unit 1 explores the basics of operating systems and operating system security, including privileged and non-privileged states, threads and processes, and memory management.

Learning Activities

u01s1 - Studies

The readings, research, and Skillsoft resources in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 1, "Security in the Microsoft Windows Operating System", pages 1–9.
- Chapter 2, "Basic Components of Linux Security", pages 22–27

Research

Internet and Library Research

Use the following keywords to research concepts related to operating system and operating system security specific to various components of the operating system:

- Operating system privileged state.
- Operating system non-privileged state.
- Operating system threads and processes.
- Operating system threads.
- Operating system processes.
- Operating system real memory.
- Operating system virtual memory.
- Operating system memory management.
- Operating system virtual memory management.

Using the internet, view:

- USENIX Association. (2012). Ask WINE: Are we safer today? Evaluating operating system security [Video] (31 min.) | Transcript. Retrieved from https://www.usenix.org/conference/leet12/workshop-program/presentation/dumitras

Skillsoft Resources

- Skillsoft. (n.d.). Security+: Operating System Security Considerations [Video]. (7 min.)
- Skillsoft. (n.d.). Microsoft Security Fundamentals: Operating System Security [Tutorial]. (1 hour 40 min.)

Optional Readings

Smith, R. W. (2012). *Linux essentials*. Indianapolis, IN: Sybex Inc.

- Chapter 1, "Selecting an Operating System," pages 1–20.
- Chapter 2, "Investigating Linux's Principles and Philosophy," pages 21–32.

Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information systems security professional study guide* (6th ed.). Indianapolis, IN: Wiley.

- Chapter 11, "Principles of Security Models, Design and Capabilities," pages 447–476.

- Chapter 12, "Security Architecture Vulnerabilities, Threats, and Countermeasures," pages 477–530.

u01s1 - Learning Components

- Describe various operating system security processes.

u01s2 - Software Preparation and Technology Access

In this course, you will be using software and technology that is needed to complete designated activities and assignments. There is no additional cost for this software and technology. Some software packages will be made available to you at no additional cost through Capella's subscription with Microsoft, while other software packages are available for free download through open-source licensing.

Capella University requires learners to meet certain minimum computer requirements. Please note that some software required for a course may exceed these minimum requirements. Check the requirements for the software you may need to download and install to make sure it will work on your device. Most software will require a Windows PC. If you use a Mac, refer to Installing a Virtual Environment and Windows on a Mac.

Additional Online Resources

Note: As a Capella learner, you have access to IT online resources through Capella's Skillsoft subscription, where you can find helpful materials.

u01v1 - Lab: Implementing Access Controls with Windows Directory

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u01v1 - Learning Components

- Identify various authentication methods.

u01v2 - Lab: Installing a Core Linux Operating System on a Server

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u01v2 - Learning Components

- Describe various operating system security processes.

u01d1 - Operating System Design and Vulnerabilities

Microsoft Windows has been the market leader in operating systems for desktops and servers for decades; however, that is not the whole story in the operating system arena. UNIX, LINUX, and other "NIX" variants also have areas where they are more dominant, such as Apache servers that connect organizations to the Internet; the Cisco IoS operating system that runs routers, switches, and an array of networking devices; and mobile devices that run on Android and Apple operating systems. This new diversity of operating systems (in particular, the rise of Apple has kicked up turf wars) has created some shift in the focus of attackers. Prior to these developments, Windows was politically unpopular and far ahead in market share, making them the target of the majority of malware writers and other intrusions.

Select an operating system of your choices to focus on in this discussion. Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following topics:

- Describe your particular operating system selection including the niche that it fills in the operating system market.
- Describe the threats and vulnerabilities that are most commonly associated with a particular operating system.
- Explain the security implications related to the concepts of privileged and non-privileged states as a function of an operating system.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u01d1 - Learning Components

- Describe various operating system security processes.
- Apply skills in critical thinking, APA formatting, and writing.

u01d2 - Operating System Processes, Threads, and Memory

One of the selling points for early versions of Windows was the ability that it had to leverage threads to allow users to do more than one activity at a time. Prior to this ability, computers were limited in the ability to multitask. Understanding how threads and processes work as a function of the operating system is important foundational information to understanding how threats can exploit those functions or what the potential vulnerabilities might be.

Many organizations have had the misfortune of experiencing a denial of service attack. The technical functioning of the operating system and how memory is used are also important concepts to understand in order to fully understand the exploits that use memory to attack organizational information assets.

Select an operating system of your choices to focus on in this discussion. Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following topics:

- Describe how threads and processes work in an operating system including what they contribute to the overall functionality of the operating system.
- Describe the threats and vulnerabilities that are most commonly associated with threads and processes specific to a particular operating system.
- Explain the basics of virtual and real memory and what aspects of memory are the point of vulnerability for an attacker.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u01d2 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.

Unit 2 >> Access Control and Authentication Strategies and Tools

Introduction

Unit 2 focuses on authentication and access controls including file systems, isolation, separation, and encapsulation.

Learning Activities

u02s1 - Studies

The readings and research in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Reading

The required reading covers access control and authentication activities, and tools and procedures which support completion of the unit assignment and discussion.

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 3, "Access Controls in Microsoft Windows," pages 50–76.
- Chapter 4, "User Privileges and Permissions," pages 80–108.

Internet Research

Internet and Library Research

Use the following keywords to engage in Internet and library research:

- Information security access controls.
- Computer security access controls.
- Information security authentication methods.
- Computer security authentication methods.
- Information security file systems.
- Computer security file systems.
- Information security domain separation.
- Computer security domain separation.
- Information security process isolation.
- Computer security process isolation.
- Information security resource encapsulation.
- Computer security resource encapsulation.

Optional Reading

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (2nd ed.). Boston, MA: Elsevier Science.

- Chapter 2, "Identification and Authentication," pages 23–38.
- Chapter 3, "Authorization and Access Control," pages 39–56.

Gibson, D. (2011). *Microsoft Windows security: Essentials*. Indianapolis, IN: Wiley Publishing.

- Chapter 3, "Understanding User Authentication," pages 43–68.
- Chapter 4, "Securing Access with Permissions," pages 69–94.

Mansfield-Devine, S. (2010). Security through isolation. *Computer Fraud & Security, 2010*(5), 8–11.

u02s1 - Learning Components

- Identify various authentication methods.
- Identify controls to protect various file systems.
- Describe control list functionality.
- Identify different file systems.

u02v1 - Lab: Using Access Control Lists to Modify File Permissions on Windows Systems

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u02v1 - Learning Components

- Identify various authentication methods.
- Describe control list functionality.

u02v2 - Lab: Hardening Security With User Accounts Management and Security Controls

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u02v2 - Learning Components

- Identify various authentication methods.
- Describe control list functionality.

u02a1 - Access Control and Authentication Methods and Models

Instructions

Access controls and authentication systems are some of the most ubiquitous of all information security controls. Too often these controls still hinge on poorly implemented and managed password strategies. However, there is a wide array of technologies and tools available to organizations seeking to secure their information assets. As governments create more regulations and organizations experience larger and more widely publicized breaches of personal data, these organizations may more frequently turn to additional layers of controls to supplement traditional access and authentication strategies.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Write a 2–3 page paper that covers the following topics:

- Describe your lab experiences related to access controls and authentication systems available for use in organizations to protect information assets.
- Analyze the security characteristics of commonly used file systems.
- Explain how access control lists play a role in a layered network security strategy.
- Explain the security benefits available through domain separation, process isolation, resource encapsulation, and least privilege.

At the end of your paper, also include lab screenshots from u01v1 and u02v1.

Additional Requirements

Your assignment should also meet the following requirements:

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Your paper should demonstrate current APA style and formatting.
- **Number of resources:** Include a minimum of three resources, appropriately cited throughout your paper and in your reference list.
- **Suggested length:** 2–3 pages, typed and double-spaced, not including the title page and reference list.
- **Font and font size:** Times New Roman, 12 point.

Submit your paper including lab screen shots to the assignment area.

Course Resources

APA Style and Format

u02d1 - Characteristics of Access Control and Authentication

Most IT and IAS professionals are familiar with the basic concepts surrounding authentication and access control systems. There are fewer professionals who have taken the time to consider the more granular characteristics of these controls and the options that are available for differentiation, selection, and implementation.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Describe the combination of authentication and access controls that you believe best balance cost, complexity, and security. Support your position.
- Explain how domain trusts, isolation technologies, and the separation and organization of those technologies can support a network security strategy.
- Describe an example of how encapsulation or encryption contribute to a specific access control or authentication solution.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u02d1 - Learning Components

- Describe various operating system security processes.
- Identify various authentication methods.
- Apply skills in critical thinking, APA formatting, and writing.

Unit 3 >> Application Security Basics

Introduction

Application security has become a critical aspect of information security, with a high percentage of exploits occurring by leveraging defects in computer code. Unit 3 explores some of the specific areas of vulnerability within applications, examples of how those vulnerabilities can be exploited, and some of the mitigations available to prevent or reduce the risk of those exploits.

Learning Activities

u03s1 - Studies

The readings and research in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

The required reading covers vulnerabilities specific to Web-based applications and browsers and strategies to mitigate some of those vulnerabilities, and will support completion of the unit discussions.

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 5, "Microsoft Application Security," pages 111–113.
- Chapter 6, "Networked Application Security," page 138.

Use the Capella Library to read:

- Stuttard, D., Pinto, M. (2011). *The web application hacker's handbook: Finding and exploiting security flaws* (2nd ed.). Indianapolis, IN: Wiley.
  - Chapter 1, "Web Application (In)Security," pages 1–16.
  - Chapter 2, "Core Defense Mechanisms," pages 17–38.
  - Chapter 12, "Attacking Users: Cross Site Scripting," pages 431–500.

Use the Internet to view:

- CernerEng. (2014). *Application security - Understanding, exploiting, and defending against top web vulnerabilities* [Video] | Transcript. Retrieved from http://www.youtube.com/watch?v=sY7pUJU8a7U (57 min.)

Research

Internet and Library Research

Use the following keywords and research application security concepts

- SQL Injection.
- Cross-Site Scripting.
- Buffer Overflow Attacks.
- Denial of Service Attacks.
- Distributed Denial of Service Attacks.
- Internet browser security.
- Object based code.
- Object oriented code.
- Application security controls.
- Application security mitigations.
- Computer code review.
- Computer code testing tools.

Optional Readings

Zalewski, M. (2012). *The tangled web: A guide to securing modern web applications*. San Francisco, CA: No Starch Press.

- Chapter 9, "Content Isolation Logic," pages 141–164.
- Chapter 10, "Origin Inheritance," pages 165–172.

u03s1 - Learning Components

- List the steps of the information flow from database server to application.

u03v1 - Lab: Hardening Windows Server Security Using Microsoft Baseline Security Analyzer

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u03v1 - Learning Components

- Identify database security issues.

u03v2 - Lab: Hardening Security for Linux Services and Applications

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u03v2 - Learning Components

- Identify database security issues.

u03d1 - Application Development Security Implications

Application security is one of the primary avenues used by attackers to penetrate systems and networks. Some of these avenues still being exploited have been known for decades. There has historically been a wide gap between application developers and security professionals—a gap that more organizations are becoming motivated to bridge.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Differentiate between object-based and object-oriented computer code.
- Identify common avenues of vulnerability specific to application security.
- Explain strategies that mitigate application security vulnerabilities.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u03d1 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.

u03d2 - Secure Coding Practice Recommendations

Tasty Cookie CIO, Joan Thompson, attended a meeting of the local chapter of the Information Security Systems Association (ISSA) where a presenter demonstrated common attack vectors, including how to exploit code flaws to perform SQL injection to alter data in a backend database, and how failure to properly define data elements can result in buffer overflows. Joan had previously been relatively disengaged on the topic of application security because the primary applications used to run core business processes are all COTS (commercial off the shelf) applications that had regular patching and version control procedures in place. Following the demonstrations, she became aware of the threats specific to Web-based applications and returned to the office determined to look more deeply into the marketing and Web-based services that are being used to promote the organization.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Explain buffer overflows.
- Explain SQL injection.
- Explain cross-site scripting.
- Describe a strategy the CIO can follow to ensure secure coding practices are implemented that prevent Web-based attacks.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u03d2 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.
- Identify database security issues.

Unit 4 >> Database Security

Introduction

Database design and development includes decision points that have security implications. Unit 4 will focus on the specific ways that databases can be exploited and the tools that are available to mitigate those potential vulnerabilities.

Learning Activities

u04s1 - Studies

The readings, research, and Internet resources in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

Taylor, A. G. (2013). *SQL for dummies*. Hoboken, NJ: Wiley.

- Chapter 14, "Providing Database Security," pages 297–312.
- Chapter 15, "Protecting Data," pages 313–332.

Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information systems security professional study guide* (6th ed.). Indianapolis, IN: Wiley.

- Chapter 7, "Software Development Security," pages 275–326.

Research

Internet and Library Research

Use the following keywords to engage in research on databases and database security:

- Database and server interfaces security factors.

- NoSQL Security vulnerabilities.
- Common DBMS security models.
- Database indexing security factors.
- Database aggregation security factors.
- Database polyinstantiation security factors.
- Database inference security factors.

Use the Internet to read:

- w3resource (2018). NoSQL Introduction. Retrieved from https://www.w3resource.com/mongodb/nosql.php

Optional Skillsoft Resources

- Skillsoft. (n.d.). Security+: Database Security [Video]. (1 min.)
- Skillsoft. (n.d.). CSSLP: Database Security [Video]. (5 min.)

u04s1 - Learning Components

- List the steps of the information flow from database server to application.
- Identify database security issues.
- Describe relationships between database servers and applications.
- Identify common database security models.
- Describe a No SQL Database.

u04v1 - Lab: Perform a Web Site and Database Attack by Exploiting Identified Vulnerabilities

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u04v1 - Learning Components

- List the steps of the information flow from database server to application.
- Identify database security issues.
- Describe relationships between database servers and applications.
- Identify common database security models.
- Describe a No SQL Database.

u04a1 - Database Security Characteristics and Tools

Instructions

Timbuktu Tailors opened their doors in 1995 to provide the service of tailoring and repairing clothing for the community surrounding the shop. The family who opened Timbuktu Tailor used paper records to keep track of the finances for the company, which has worked well over the years. Last year, Tony Timbuktu was advised by his tax accountant that with the growth of the business, the practice of paper record-keeping was becoming increasingly less viable. Tony was advised to consider adapting the finances of the business to an electronic application and database. Tony began doing research of the alternatives that are available to him and became quickly overwhelmed. You were hired to help Tony sort through the pros and cons of the options that are available to him.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Write a 2–3 page paper that covers the following:

- Consider an outsourced solution for record keeping; what are the security implications for the flow of data between the shop and the servers located in an offsite location?
- Compare and contrast the differences in selecting an SQL versus a NoSQL database within the context of a small business application.
- Evaluate the potential vulnerabilities that are common to DBMS and databases which are important to consider as part of selection of these technologies.
- Describe database security issues related to indexing, aggregation, polyinstantiation, and inference and how they might impact purchase and implementation of a database in the context of a small business.

At the end of your paper, also include lab screenshots from u04v1.

Additional Requirements

Your assignment should also meet the following requirements:

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Your paper should demonstrate current APA style and formatting.
- **Number of resources:** Include a minimum of three resources, appropriately cited throughout your paper and in your reference list.
- **Suggested length:** 2–3 pages, typed and double-spaced, not including the title page and reference list.
- **Font and font size:** Times New Roman, 12 point.

Submit your paper including lab screen shots to the assignment area.

Course Resources
APA Style and Format
SQL for Dummies

u04d1 - Database Security Controls

Database security can be a very complicated business. There are many different forms of database using many different languages as a foundation. Databases are implemented in a variety of environments and contexts. This highly variable context related to database implementation means that security professionals are required to consider the risks to database security within the specific context; however, there are some security threats and mitigating controls that are common across database solutions. These common approaches to database security are known as security models. For example, access controls, physical security, remote access security, and monitoring of privileged accounts are all examples of threats common across database solutions that require appropriate mitigations.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- What are some examples of security models that can be used to support database security?
- Describe a strategy that database administrators can use to ensure that applications used to enter data into databases cannot be used to exploit that data.
- Explain strategies that mitigate common database security vulnerabilities.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u04d1 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.
- Identify database security issues.
- Identify common database security models.

Unit 5 >> Operating System Security Mitigations

Introduction

There are both internal and external factors that play a role in the security level of operating systems. Among the internal considerations are controlling available ports and services through operating system hardening. External considerations include the creation and enforcement of information security policies, application of system patches, and updating versions of the operating system to ensure the production version is fully supported by the manufacturer of that operating system. Unit 5 explores strategies for enhancing and mitigating risk to information assets through exploitation of operating system flaws and vulnerabilities.

Learning Activities

u05s1 - Studies

The readings, research, and Internet resources in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

The required reading covers tools and resources available to mitigate vulnerabilities to information assets created by operating systems which will support completion of the unit discussion

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 7, "Hardening the Microsoft Windows Operating System," pages 174–203.
- Chapter 8, "Kernel Security Risk Management," pages 206–237.

Research

Internet and Library Research

Use the following keywords to research concepts related to operating security controls and mitigations:

- Operating system security controls.
- Operating system security mitigations.
- Operating system vulnerability patching.
- Operating system updates.
- Operating system port security.
- Operating system hardening.
- Operating system security policy.

Use the Internet to view:

- CUFP 2013. (2013). CUFP 2013: Tom Hawkins: Redesigning the computer for security [Video] | Transcript. *Commercial Users of Functional Programming (CUFP)*. Retrieved from http://cufp.org/2013/tom-hawkins-bae-systems-redesigning-computer-secur.html (26 minutes).

Optional Readings

Calerdon Pale, P. (2012). *Nmap 6: Network exploration and security auditing cookbook*. Birmingham, AL: Packt Publishing.

- Chapter 1, "Nmap Fundamentals," pages 9–44.
- Chapter 2, "Network Exploration," pages 45–76.

Carpenter, T. (2012). *Microsoft windows operating system: Essentials*. Hoboken, NJ: Sybex.

- Chapter 15, "Windows Update," pages 327–342.

u05s1 - Learning Components

- Describe control types.
- Describe the function of updates and patches.
- Describe components of a security policy.

u05v1 - Lab: Identifying and Removing Malware From Windows Systems

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u05v1 - Learning Components

- Describe control types.
- Describe the function of updates and patches.
- Describe controls specific to application security.

u05v2 - Lab: Securing Servers with the Security Configuration Wizard and the Windows Firewall

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u05v2 - Learning Components

- Describe control types.
- Describe controls specific to application security.

u05v3 - Lab: Hardening Security for the Linux Kernel

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u05v3 - Learning Components

- Describe control types.
- Describe controls specific to application security.

u05d1 - Operating System Security Mitigations

One of the foundational tenets of information security is the concept of layering security controls with the idea that there is an incremental gain with each layer providing heightened security not present with the implementation of each of the individual controls. For example, implementing user accounts and passwords is a mitigation to the risk to assets caused by operating system vulnerabilities. Implementing user accounts and password and adding group policies that control what those users can do with their accounts further decreases the risk and enhances the mitigation of the vulnerabilities.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following topics:

- Describe categories of controls that are available to implement as layered security to mitigate risks to information assets due to operating system vulnerabilities.
- Describe controls and resources that are specific to vulnerability patching and version management.
- Describe how management of ports and services can mitigate the risk to information assets as part of an operating system security plan.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u05d1 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.
- Describe control types.
- Identify different IT security policies that would affect application security.
- Describe the function of updates and patches.

u05d2 - Application of Operating System Security Controls

Peter Parker is the new network administrator for a local clothing store in downtown St. Paul. One of the first tasks that Peter engages in is to review existing information security policy. He discovers that there are a number of usage policies about what is acceptable use of host computers by users; however, there is no policy that provides necessary guidance to IT staff that will help them understand the priorities of the leadership of the store. Peter convenes a meeting with these leaders and discusses with them the need to determine what

information assets are important to the organization so that he can use those priorities to develop information security policies needed to perform the rest of his tasks.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Describe the role that operating system security policy plays in supporting selection, implementation, and maintenance of operating system security controls.
- Explain how articulation of the priorities of an organization translates into operating system controls.
- Identify operating system controls that are used to protect those information assets that an organization determines are critical to the success of the business.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u05d2 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.
- Identify different IT security policies that would affect application security.
- Describe controls specific to application security.

Unit 6 >> Application Security Controls and Tools

Introduction

The development, selection, implementation, and maintenance activities for software include facets that are common across all forms of software. Unit 6 covers the controls that are available to mitigate vulnerabilities to information assets created by common software vulnerabilities.

Learning Activities

u06s1 - Studies

The readings and Skillsoft resources in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

The required reading focuses on controls that are available to mitigate software vulnerabilities that can put at risk the information assets for an organization, which will support completion of the unit assignment and discussion.

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 6, "Networked Application Security," pages 138–170.
- Chapter 9, "Best Practices for Microsoft Windows and Application Security," pages 240–254.

Skillsoft Resources

- Skillsoft. (n.d.). CompTIA CASP CAS-002: Application Vulnerabilities and Security Controls [Tutorial]. (1 hour 41 minutes).

Optional Readings

Dulaney, E. A. (2011). *CompTIA security+ study guide: Exam SY0-301*. Indianapolis, IN: Sybex.

- Chapter 7, "Operating System and Application Security," pages 245–290.

Nahari, H., & Krutz, R. L. (2011). *Web commerce security: Design and development*. Indianapolis, IN: Wiley.

- Chapter 6, "System Components: What You Should Implement," pages 193–244.
- Chapter 7, "Trust But Verify," pages 245–266.

Use the Internet to review:

- CernerEng. (2014). Application security - Understanding, exploiting, and defending against top web vulnerabilities [Video] | Transcript. (57 minutes).

u06s1 - Learning Components

- Describe control types.
- Describe the function of updates and patches.
- Describe controls specific to application security.

u06v1 - Lab: Securing Internet Client Server Applications on Windows Systems

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u06v1 - Learning Components

- Describe control types.
- Describe the function of updates and patches.
- Describe controls specific to application security.

u06v2 - Lab: Applying Best Practices for Security Software Management

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.

- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u06v2 - Learning Components

- Describe control types.
- Describe the function of updates and patches.
- Describe controls specific to application security.

u06a1 - Application of Software Security Controls

Instructions

Tom Tanner is an external auditor doing an audit on a business line of a multi-national corporation. He discovers as part of this audit that this business line was recently acquired by the parent company. The long term intent is to convert this business to the corporate ERP system, however the existing ERP system is custom built software that is maintained by internal developers hired by the business line for this purpose. Tom is accustomed to auditing organizations that use COTS (commercial off the shelf) applications that have predictable and determinable vulnerability and version patching controls and procedures. He hires you to function as a sub-contractor to audit the security implications of this customized ERP software.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Describe the security controls that are in place, i.e. controls that mitigate application threats and vulnerabilities, both in terms of the development and the use of the software.
- Describe the role that existing application security policy will play in ensuring that the audit covers the appropriate software development and maintenance controls.
- Explain how to audit the software patching and version control process that is performed internal to the organization.
- Describe how to approach audit recommendations for missing application controls related to a system known to be at the end of the useful lifecycle.
- Apply mitigations that support application security within a specific organization.

At the end of your paper, also include lab screenshots from u06v1 and u06v2.

Additional Requirements

Your assignment should also meet the following requirements:

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Your paper should demonstrate current APA style and formatting.
- **Number of resources:** Include a minimum of three resources, appropriately cited throughout your paper and in your reference list.
- **Suggested length:** 2–3 pages, typed and double-spaced, not including the title page and reference list.
- **Font and font size:** Times New Roman, 12 point.

Submit your paper including lab screen shots to the assignment area.

Course Resources

APA Style and Format

u06d1 - Application Security Basics

The CIO and the marketing vice president of Nancy's Noodle Factory have been having a heated debate about allowing marketing staff to integrate the company Twitter feed into the company Web site. Nancy Nelson, the CEO and owner of the company, listened to both positions and charges you with figuring out how to meet the marketing department's objectives in a way that accommodates the security concerns of the CIO.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Describe the Web development controls that you recommend be implemented.
- Explain the security controls that will be used to prevent any part of the Web hosting assets from being compromised.
- Identify auditing strategies that can be followed to ensure that the development and hosting components are following the agreed upon strategies.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources

Undergraduate Discussion Participation Scoring Guide

Application Security – Understanding, Exploiting, and Defending Against Top Web Vulnerabilities [Video]

u06d1 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.
- Describe control types.
- Describe controls specific to application security.

Unit 7 >> Encryption as a Component of Security Controls

Introduction

Encryption is a mathematical solution to obscuring data and protecting data from exposure to unauthorized recipients. Encryption is not a means to an end, but is rather a component of a variety of information security controls. Encryption is not a single solution, but a variety of approaches to accomplishing the goal of data protection. Unit 7 explores the ways in which encryption can be used to support application and operating system security.

Learning Activities

u07s1 - Studies

The readings and research in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

The required reading covers encryption concepts which will support completion of the unit discussions.

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 10, "Microsoft Windows Encryption Tools and Technologies," pages 257–278.
- Chapter 11, "Cryptography," pages 282–317.

Research

The Internet resources cover facets of encryption and the role it plays in application and operating system security, which will support completion of the unit discussions.

Internet and Library Research

Use the following keywords to research encryption related concepts:

- Encryption for computer interfaces.
- Encryption data in transit.
- Encryption data at rest.
- Encryption hashing.
- Encryption inference.
- Encryption aggregation.
- Encryption collisions.
- Encryption history.

Optional Readings

Konheim, A. G. (2010). *Hashing in computer science: Fifty years of slicing and dicing*. Hoboken, NJ: Wiley-Blackwell.

- Chapter 6, "Basic Concepts of Cryptography," pages 94–116.
- Chapter 7, "Basic Concepts," pages 117–123.
- Chapter 8, "Hash Functions," pages 124–131.
- Chapter 9, "Hashing Functions: Examples and Evaluation," pages 132–140.

Hoffstein, J., Pipher, J. C., & Silverman, J. H. (2008). *An introduction to mathematical cryptography*. New York, NY: Springer.

- Chapter 1, "An Introduction to Cryptography," pages 1–58.

u07v1 - Lab: Configuring Bitlocker and Windows Encryption

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u07v1 - Learning Components

- Describe different threats and vulnerabilities of data in the cloud.

u07v2 - Lab: Using Encryption to Enhance Confidentiality and Integrity

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u07d1 - Encryption as a Component of Operating System Security

Encryption is used in a variety of ways to support different aspects of operating system security. One important example is the use of encryption to prevent passwords being transmitted across the network from being compromised by anyone able to monitor packets on the network.

Use the study materials and engage in any research necessary to fill in knowledge gaps. Discuss the following:

- Identify an operating system security control that uses encryption as a functional component of the control.
- Describe how encryption contributes to the successful operation of the operating system control.
- Identify how encryption can be used to defeat exploits that use inference and aggregation to identify patterns in traffic.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u07d1 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.
- Describe different threats and vulnerabilities of data in the cloud.

u07d2 - Evolution of Encryption

Cryptography has been around since ancient times, when coded messages were sent by courier from sender to recipient. Modern encryption uses mathematical algorithms as the basis for how it functions; however, as computing power increases the need for more robust encryption has been the hallmark of that evolution. Common encryption solutions have much larger key lengths as one of the enhancements over earlier solutions such as DES.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Describe the primary differences that have occurred in the evolution of encryption from DES through AES.
- Explain one political controversy involving encryption that is a part of the historical evolution of encryption.
- Determine strategies to ensure that encryption is used appropriately to protect operating system and application security within an organization.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u07d2 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.

Unit 8 >> Virtualization and Cloud Computing Security

Introduction

An increasing number of organizations have opted to leverage some of the benefits of virtualization and cloud computing. Some of the earlier limitations to virtualization in terms of scalability have been resolved, and the benefits of being able to pull down a failed virtual host and quickly replace it with a new host is important to organizations who see the cost of having workers idled by non-functioning technologies. Unit 8 explores virtual and cloud computing options and the related vulnerabilities and controls that are available to mitigate those vulnerabilities.

Learning Activities

u08s1 - Studies

The readings, research, and Skillsoft resources in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

Ottenheimer, D., & Wallace, M. (2012). *Securing the virtual environment: How to defend the enterprise against attack*. Indianapolis, IN: Wiley.

- Chapter 1, "Virtualized Environment Attacks," pages 1–40.
- Chapter 5, "Abusing the Hypervisor," pages 141–184.

Required Skillsoft Resources

- Skillsoft. (n.d.). Cloud Computing Fundamentals: Virtualization and Data Centers [Tutorial]. (1 hour 23 minutes).
- Skillsoft. (n.d.). CompTIA CASP CAS-003: Integrating Cloud and Virtualization Technologies in the Enterprise [Tutorial]. (44 minutes).
- Skillsoft. (n.d.). CompTIA Security+ 2011: Securing Applications, Virtualization, and Cloud Computing [Tutorial]. (2 hours).

Research

The Internet resources cover security vulnerabilities specific to the hypervisor and virtualized environments, which will support completion of the unit assignment and discussion.

Internet and Library Research

Use the following keywords and engage in research of security concepts related to virtual and cloud computing:

- Virtual computing security.
- Cloud computing security.
- Hypervisor security.
- Virtual computing security tools.
- Cloud computing security tools.
- Security vulnerabilities of virtual computing.
- Security vulnerabilities of cloud computing.

u08s1 - Learning Components

- Describe different threats and vulnerabilities of data in the cloud.
- Define virtualization and cloud computing.
- Define hypervisor.
- Describe the difference between public and private clouds.

u08a1 - Application of Virtual and Cloud Computing Security

Instructions

Dr. David Nelson is the managing partner in a small clinic practice located in southern California. He and his eight partners have been exploring the benefits of participating in the federal meaningful use incentives that would mean collecting tens of thousands of dollars in exchange for implementing an electronic health record to replace their existing paper files. Dr. Nelson is concerned at the cost of adding sophisticated technology into the overall management responsibilities, as well as the ability to find and retain expensive IT support staff sufficiently knowledgeable and available to meet their needs. Dr. Nelson attends the annual HIMSS conference where he has the opportunity to speak to a large number of vendors and peers about options available to him, and has returned from the conference convinced that the optimal approach for him and his partners is to purchase a cloud computing "Software as a Service" solution. One of this partners is not as convinced and has asked you to attend their next partners meeting to discussion security and privacy implications and to recommend solutions they might consider to manage having their regulated patient data stored offsite with a cloud provider.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Describe the potential security and privacy implications of storing patient data in a 3rd party controlled cloud environment.
- Explain the role of the hypervisor and the security vulnerabilities specific to this technology.
- Identify tools that are available to mitigate vulnerabilities specific to virtual and cloud computing implementations.
- Recommend how a small medical clinic can leverage cloud computing strategies without putting their patient data at risk.
- Describe the implications of public versus private clouds in operating system security.

Additional Requirements

Your assignment should also meet the following requirements:

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Your paper should demonstrate current APA style and formatting.
- **Number of resources:** Include a minimum of three resources, appropriately cited throughout your paper and in your reference list.
- **Suggested length:** 2–3 pages, typed and double-spaced, not including the title page and reference list.
- **Font and font size:** Times New Roman, 12 point.

Submit your paper to the assignment area.

Course Resources

APA Style and Format

u08d1 - Virtual Environments

Not all virtualized environments are hosted in the cloud. Many organizations have chosen to leverage the use of virtual hosts and servers that are managed internally.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Describe the security-related benefits to implementing virtualized environments that are managed internal to an organization.
- Identify any security-related challenges specific to implementing virtualized environments that are managed internal to an organization.
- Explain the tools that are available to network administrators who want to securely manage virtual host and servers internal to the organization.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u08d1 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.
- Describe different threats and vulnerabilities of data in the cloud.
- Define virtualization and cloud computing.
- Define hypervisor.
- Describe the difference between public and private clouds.

Unit 9 >> Windows Operating System Disaster Recovery Components

Introduction

Windows operating systems contain a number of components that support fault tolerance and disaster recovery. Among those components are RAID, power management, and data backup functionality. Unit 9 focuses on

these components and how they play a role in preventing loss of data or worker productivity due to failed technology.

Learning Activities

u09s1 - Studies

The readings and research in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

The required reading covers fault tolerance and disaster recovery components that exist as part of the Windows operating systems, which will support completion of the unit discussions.

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 12, "Microsoft Windows Backup and Recovery Tools," pages 320–346.
- Chapter 13, "Microsoft Windows Incident Handling and Management," pages 349–370.

Research

The Internet resources cover fault tolerance and disaster recovery components of Windows operating systems and will support completion of the unit discussions.

Internet and Library Research

Use the following keywords to research concepts related to Windows disaster recovery components:

- Windows operating system power management.
- Windows server power management redundancy.
- Windows server power management fault tolerance.
- Windows server power management disaster recovery.
- Windows server RAID configuration.
- RAID disaster recovery.
- RAID fault tolerance.
- RAID data security.
- Active Directory disaster recovery.
- Active Directory fault tolerance.
- Active Directory redundancy.

Use the internet to view:

- Microsoft TechEd North America. (2012). The evolution of active directory recovery [Video] | Transcript. Retrieved from https://channel9.msdn.com/Events/TechEd/NorthAmerica/2012/SIA319. (79 minutes).

Optional Readings

Johnson, S. (2010). *Mastering Microsoft Windows Small Business Server 2008*. Indianapolis, IN: Wiley.

- Chapter 8, "Backing Up and Performing Disaster Recovery," pages 195–216.
- Chapter 12, "Storage Management," pages 255–276.
- Chapter 14, "Backup and Recovery," pages 307–326.

Panek, W. (2011). *Microsoft Windows 7 administration instant reference*. Indianapolis, IN: Wiley.

- Part IV, "Recovery," pages 531–576.

u09s1 - Learning Components

- Identify the different types of system logs.

u09v1 - Lab: Creating a Scheduled Backup and Replicating System Folders

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u09d1 - Fault Tolerance in Windows Operating Systems

Disk configuration and power management are two of the fault tolerant components within a Windows environment meant to reduce the risk of lost data and worker productivity due to system failures.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Explain how RAID configuration and other disk management strategies contribute to the fault tolerance of Windows environments.
- Explain how power management and configuration can contribute to reduced risk of data loss and lost worker productivity.
- Describe the wisdom of using the data backup features contained as part of the Windows operating system as opposed to purchasing third party tools to complete that work.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u09d1 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.

u09d2 - Active Directory Recovery

Active Directory is another aspect of the Windows environment that includes components intended to enhance fault tolerance and support disaster recovery. Al Smith is the CIO of a small manufacturing plant. The executive committee has charged him with engaging in disaster recovery drill planning. Al knows about some of the DR tools that are native to the Windows environment, but he is not as knowledgeable about the tools contained within Active Directory. You are hired to provide Al with an update as to how Active Directory components can be integrated into an overall disaster recovery plan.

Use the study materials and engage in any research needed to fill in knowledge gaps. Discuss the following:

- Describe the components within Active Directory that play a role in fault tolerance and disaster recovery.
- Identify any critical procedures or policies that must be created to support recovery of Active Directory as part of a disaster recovery planning drill.
- Explain any third party tools that may contribute to disaster recovery of a Windows environment.

Response Guidelines

Read the posts of your peers and respond to two (minimum), expanding on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Undergraduate Discussion Participation Scoring Guide
The Evolution of Active Directory Recovery [Video] | Transcript

u09d2 - Learning Components

- Apply skills in critical thinking, APA formatting, and writing.

Unit 10 >> Operating System Logging and Auditing

Introduction

Information security has a set of rules about how and when to apply mitigations. There is a recognition that if systems were sufficiently concerned to eliminate all of the potential risk to security, the systems would be essentially unusable. Application of optimal controls means achieving the proper balance between cost, availability, and security. This balance sometimes means that availability takes precedence, meaning that security controls are weaker than desired. The mitigation for the need to use weaker than desired controls is to enhance those controls with the addition of auditing and monitoring tools. Operating system and Active Directory logs can be useful in conducting controls audits and in providing an additional layer of governance and oversight. Unit 10 focuses on auditing and logging as a component of operating systems.

Learning Activities

u10s1 - Studies

The readings resources in this unit contain information that will support the completion of the unit discussions, labs, and assignments.

Readings

The required reading covers auditing and logging features available in Windows environments that contribute to the overall security profile of the systems, and supports completion of the unit assignment and discussion.

Capella University (2018). *Capella University IT 4080*. Burlington, MA: Jones & Bartlett Learning.

- Chapter 14, "Microsoft Windows Security Profile and Audit Tools," pages 373–398.
- Chapter 15, "Information Systems Audit Requirements," pages 401–435.

Optional Readings

Tuli, P. & Sahu, P. (2013). System monitoring and security using keylogger. *International Journal of Computer Science and Mobile Computing, 2*(3), 106–111.

Hingarh, V., & Ahmed, A. (2013). *Understanding and conducting information systems auditing*. Singapore: Wiley.

- Chapter 1, "Overview of Systems Audits," pages 3–16.
- Chapter 4, "Information Systems Audit Requirements," pages 59–70.
- Chapter 5, Conducting an Information Systems Audit," pages 71–100

Optional Skillsoft Resources

- Skillsoft. (n.d.). CSSLP: Logging and Auditing [Video]. (6 minutes).
- Skillsoft. (n.d.). CompTIA CASP CAS-002: System, Audit, and Review Logs [Video]. (5 minutes).

u10s1 - Learning Components

- Describe operating system audit tools.
- Identify the different types of system logs.
- Describe the function of the operating system log.
- Describe the logs used to monitor users.
- Describe operating system logging tools.
- Identify monitoring techniques.
- Define a baseline.

u10v1 - Lab: Protecting Digital Evidence, Documentation, and The Chain of Custody

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u10v1 - Learning Components

- Describe operating system audit tools.
- Describe the logs used to monitor users.
- Describe operating system logging tools.

u10v2 - Lab: Applying Best Practices for Security Logging and Monitoring

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities.

Select the linked title heading above to access a lab arranged through the textbook publisher.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Screen captures from the lab.

- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing the virtual labs, contact Jones & Bartlett Technical Support:

- E-mail: support@jblearning.com
- Phone: 1-800-832-0034, option 5.

u10v2 - Learning Components

- Describe operating system audit tools.
- Identify the different types of system logs.
- Describe the function of the operating system log.
- Describe the logs used to monitor users.
- Describe operating system logging tools.
- Identify monitoring techniques.
- Define a baseline.

u10a1 - Event Logging, Auditing, and Monitoring Tools

Instructions

Jennifer Janson, the CIO of Mercy Hospital, which is a small rural hospital in Kentucky, has recently managed to hire a new medical director after two years of looking for someone to replace the last doctor. Dr. Patterson knows that he has some leverage in this situation, so one of his first demands is to reduce the access controls required by him and his part time physicians who help to staff the hospital. He makes a convincing argument for the need to be nimble in responding to critically ill patients in this new world of electronic medical records. Jennifer consults with the IT manager who functions as the information security officer for the hospital. Together they decide to cede to Dr. Patterson's request, but to mitigate this reduction in security controls by implementing a comprehensive and aggressive system logging, monitoring, and auditing program.

Use the study materials and engage in any additional research needed to fill in knowledge gaps. Discuss the following:

- Identify the events that can be captured by the operating system logs.
- Describe how to monitor the activities of logged on users.
- Describe the role of monitoring in maintaining a security baseline.
- Apply operating system audit and logging tools to meet the objectives of the auditing program.

At the end of your paper, also include lab screenshots from u10v1 and u10v2.

Additional Requirements

Your assignment should also meet the following requirements:

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Your paper should demonstrate current APA style and formatting.
- **Number of resources:** Include a minimum of three resources, appropriately cited throughout your paper and in your reference list.
- **Suggested length:** 2–3 pages, typed and double-spaced, not including the title page and reference list.
- **Font and font size:** Times New Roman, 12 point.

Submit your paper including lab screen shots to the assignment area.

Course Resources

APA Style and Format

u10d1 - Course Reflections

Share the aspects of this course that you found most useful and describe how those skills will enhance your professional goals.

Response Guidelines

You are encouraged to share with your peers how their participation has helped your understanding of the topics covered in the course, however you are not required to post responses.

Course Resources

Undergraduate Discussion Participation Scoring Guide

Scoring Guides

u02a1 - Access Control and Authentication Methods and Models Scoring Guide