Preview: IT4803 : System Assurance Security

Syllabus

Course Overview

This course introduces information security assurance concepts and practices appropriate for beginning IT professionals whose job it is to implement security strategies that protect organizations from exposure to system threats and vulnerabilities.

Topics explore ways for IT professionals to incorporate security-conscious designs for various aspects of organizational security. Labs require you to employ strategies designed to guard against hackers and viruses, and afford the opportunity for hands-on exploration of access control, authentication and encryption techniques, common methods for attacking a network system, and other related topics.

Kaltura Media

In this course, you will be required to create a presentation using Kaltura Media or similar presentation software. Refer to Using Kaltura [PDF] for more information about this courseroom tool.

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.

Disability Services

Note: If you require the use of assistive technology or alternative communication methods to participate in any course activities, please contact DisabilityServices@Capella.edu to request accommodations.

Course Competencies

(Read Only)

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

1. Apply general information assurance and security concepts.
2. Investigate security threats and system vulnerabilities.

3. Develop a security plan.
4. Design mechanisms that control unauthorized access to private information.
5. Develop a business continuity plan.
6. Interpret how information security concepts and practices are impacted by regulations and laws.
7. Communicate effectively.

Course Prerequisites

Prerequisite(s):IT3350 or IT3355.

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.

Book

Kim, D., & Solomon, M. G. (2018). *Fundamentals of information systems security* (3rd ed.). Burlington, MA: Jones & Bartlett. ISBN: 9781284116458.

Kim, D., & Solomon, M. G. (2018). *Fundamentals of information systems security* [Online labs] (3rd ed.). Burlington, MA: Jones & Bartlett. ISBN: 9781284141078.

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.

- Hendry, B. (n.d.). DevOps Fundamentals: Providing Security [Video]. Skillsoft Ireland.
- Lachance, D. (n.d.). Systems Security Certified Practitioner: Systems and Application Security [Video]. Skillsoft Ireland.
- Lachance, D. (n.d.). Vulnerabilities and Exploits [Video]. Skillsoft Ireland.
- Murphy, M. (n.d.). Implementing Disk Encryption [Video]. Skillsoft Ireland.
- Shannon, M. (n.d.). CompTIA CASP CAS-003: Organizational Security and Privacy Policies [Video]. Skillsoft Ireland.
- Shannon, M. (n.d.). CompTIA Security+ SY0-501: Types of Malware [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). Certified Ethical Hacker (CEH): Hacking Web Applications [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). CISM: Information Security Governance (Part 1) [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). CISSP 2013 Domain: Business Continuity and Disaster Recovery Planning [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). CISSP: Communication & Network Security Design [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). CISSP: Security Assessment and Testing [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). CISSP: Security Operations Part 1 [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). CompTIA Security+ SY0-401: Continuity, Disaster Recovery, and Computer Forensics [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). Microsoft Windows Server 2012 R2 - Administration: File Services and Encryption [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). Systems Security Certified Practitioner: Access Controls [Video]. Skillsoft Ireland.

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.

- Affinity Health System. (n.d.). Remote access request policy. Retrieved from http://www.affinityhealth.org/OffNav/Remote-Access-Request-Policy.htm
- AICPA. (n.d.). Segregation of duties. Retrieved from https://www.aicpa.org/interestareas/informationtechnology/resources/auditing/internalcontrol/value-strategy-through-segregation-of-duties.html
- Barth, B. (2017). The Top Cybersecurity Threats for 2017. Retrieved from https://www.scmagazine.com/the-top-cybersecurity-threats-for-2017/article/720097
- Breeden II, J. (2017). What is vulnerability management? Retrieved from https://www.csoonline.com/article/3238080/vulnerabilities/what-is-vulnerability-management-processes-and-software-for-prioritizing-threats.html
- California Hospital Association. (2016). Hospital business continuity templates: Facility-wide BCP template. [DOCX]. Retrieved from https://www.calhospitalprepare.org/sites/main/files/file-attachments/facility-wide_bcp_template.docx

- Cloud.gov. (n.d.). Continuous monitoring strategy. Retrieved from https://cloud.gov/docs/ops/continuous-monitoring/
- Giffin, R. (2015). What you need to do: Cloud computing and business continuity. Retrieved from https://perspectives.avalution.com/2015/what-you-need-to-know-cloud-computing-and-business-continuity
- Kilpatrick, I. (n.d.). Security information and event management (SIEM) systems streamline compliance. Retrieved from http://www.computerweekly.com/tip/Security-information-and-event-management-SIEM-systems-streamline-compliance
- Masters, G. (2017). Shift in password strategy from NIST. Retrieved from https://www.scmagazine.com/shift-in-password-strategy-from-nist/article/663269
- Nakashima, E. (2018). FBI chief calls encryption a 'major public safety issue.' Retrieved from https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html?utm_term=.0c5896f7198f
- National Institute of Standards and Technology. (2018). Update to cybersecurity framework. Retrieved from https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework
- NHS Digital. (2017). Encryption: example policy. [DOCX]. Retrieved from https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/encryption-guidance-for-health-and-care-organisations/encryption-example-policy
- OWASP. (2016). Testing guide introduction. Retrieved from https://www.owasp.org/index.php/Testing_Guide_Introduction
- OWASP. (2017). Web application security testing cheat sheet. Retrieved from https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet
- O'Donovan, C. (2015). SecDevOps: embracing the speed of DevOps and continuous delivery in a secure environment. Retrieved from https://securityintelligence.com/secdevops-embracing-the-speed-of-devops-and-continuous-delivery-in-a-secure-environment/
- O'Donovan, C. (2017). SecOps revisited: the challenge of DevOps for security. Retrieved from: https://securityintelligence.com/secops-revisited-the-challenge-of-devops-for-security
- Ready.gov. (n.d.). Business continuity plan. Retrieved from https://www.ready.gov/business/implementation/continuity
- SANS Consensus Policy Resource Community. (2014). Web application security policy. Retrieved from https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy
- SANS Consensus Policy Resource Community. (2014). Wireless communication policy. Retrieved from https://www.sans.org/security-resources/policies/network-security/pdf/wireless-communication-policy
- SANS Consensus Policy Resource Community. (2014). Workstation security (for HIPAA) policy. Retrieved from https://www.sans.org/security-resources/policies/server-security/pdf/workstation-security-for-hipaa-policy
- Security Intelligence. SecDevOps: Putting security at the heart of DevOps. Retrieved from https://securityintelligence.com/secdevops-putting-security-at-the-heart-of-devops/
- Shenk, J. (2013). Layered security: Why it works. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805
- SSI Staff. (2018). HID global forecasts 5 top access control trends for 2018. Retrieved from https://www.securitysales.com/access/hid-global-access-control-trends-2018
- Tischart, J. (2016). DevOpsSec, SecDevOps, DevSecOps: What's in a name? Retrieved from: https://www.csoonline.com/article/3132078/security/devopssec-secdevops-devsecops-whats-in-a-

name.html
- UAB. (2016). HIPAA core policy: Information systems and network access. Retrieved from http://www.uab.edu/policies/content/Pages/UAB-AD-POL-0000724.aspx
- United States Postal Service. (2017). Patch management process. Retrieved from https://about.usps.com/doing-business/it-policies-standards/Patch-Management-Process.htm
- Valley Medical Center. (n.d.). Valley Medical Center computing resources acceptable use policy. Retrieved from http://www.valleymed.org/vt/valley-medical-center-computing-resources-acceptable-use-policy
- Worth, T. (2018). Why endpoint management is critical to security strategy. Retrieved from https://securityintelligence.com/why-endpoint-management-is-critical-to-security-strategy
- Snell, E. (2015). Breaking down HIPAA: health data encryption requirements. Retrieved from https://healthitsecurity.com/news/breaking-down-hipaa-health-data-encryption-requirements

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.

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.

- Beyond Trust. (2017). Sample vulnerability management policy. Retrieved from https://www.beyondtrust.com/wp-content/uploads/wp-sample-vulnerability-management-policy.pdf?1446594949
- California Department of Technology. (n.d.). Incident response plan example. [DOC]. Retrieved from https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc
- Computer Security Incident Response Team. (n.d.). InfoSec password policy. [DOC]. Retrieved from http://www.csirt.org/sample_policies/sans/Password_Policy.doc
- MyPM. (n.d.). Change management plan. [DOCX]. Retrieved from http://7629-presscdn-0-90.pagely.netdna-cdn.com/wp-content/uploads/2015/02/Change-Management-Plan.docx

- South Carolina Department of Administration. (2014). Information security policy – access control. [DOCX]. Retrieved from http://www.admin.sc.gov/files/InformationSecurityPolicy-AccessControl.docx

Unit 1 >> Information Systems Security

Introduction

Implementing technical policies that align with the information security plans and “paper” policies in organizations is critical to the adoption, adherence, and compliance to those policies. While the statement of policy and the perception of governance are critical to a security program’s success, it is also necessary to have the technical controls in place that restrict and ensure users comply with the policies of the organization.

In this unit you explore the importance of security policy in an organization and implement technical policies that can have a great effect on the overall security posture of an organization.

Learning Activities

u01s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 1, "Information Systems Security," pages 2–45.

Read the following on the Internet:

- Valley Medical Center. (n.d.). Valley Medical Center computing resources acceptable use policy. Retrieved from http://www.valleymed.org/vt/valley-medical-center-computing-resources-acceptable-use-policy
  - This is a real-world example of an acceptable use policy.
- SANS Consensus Policy Resource Community. (2014). Workstation security (for HIPAA) policy. Retrieved from https://www.sans.org/security-resources/policies/server-security/pdf/workstation-security-for-hipaa-policy
  - This is a policy template for workstation security in an organization in the healthcare industry.
- National Institute of Standards and Technology. (2018). Update to cybersecurity framework. Retrieved from https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework
  - NIST framework update for cybersecurity.
- Worth, T. (2018). Why endpoint management is critical to security strategy. Retrieved from https://securityintelligence.com/why-endpoint-management-is-critical-to-security-strategy
  - This article covers the importance of security workstations and endpoints.

Skillsoft Resources

View the following Skillsoft video:

- Shannon, M. (n.d.). CompTIA CASP CAS-003: Organizational Security and Privacy Policies [Video]. Skillsoft Ireland. (40 min.).

u01s1 - Learning Components

- Read the Course Security Scenario.
- Understand the role of an acceptable use policy within an organization.
- View an example of an acceptable use policy.
- Understand the importance of workstation security.
- View an example of a workstation security policy.
- Understand the need for automated policy distribution in organizations.

u01s2 - Kaltura Media Preparation (optional)

Unit 3 and 6 assignments require you to record audio and video for a presentation. You may choose to use Kaltura Media software. Refer to the Using Kaltura [PDF] tutorial for directions on recording and submitting your recording in the courseroom.

If you have not already done so, set up and test your headset, using the installation instructions provided by the manufacturer. Then practice using it to ensure the audio quality is sufficient.

Note: If you require the use of assistive technology or alternative communication methods to participate in this activity, please contact Disability Services to request accommodations.

u01d1 - Organizational Policy

It is not uncommon to see policy development and implementation ignored in small and medium businesses (SMBs) and organizations. There could be many causes to this regardless of the impact it could have on the organization or business if there were a security incident or data breach.

Explain in your own words why you believe policy development and implementation is important in all types of organizations and businesses, regardless of size; if you believe otherwise, please explain your reasoning.

Additionally, indicate what you believe to be the risks if an organization were to have operations without technology and security policies in place.

Response Guidelines

Comment on the posts of at least two other learners.

A Note About Discussions in This Course:

The content topic should determine the length of your post; however, a minimum of 150 words is recommended. Refer to the Discussion Participation Scoring Guide for posting expectations. **Make your initial posts early in the week** to allow sufficient time for peers to respond. The expectation within the course discussions is to respond to at least two other learners by the end of the unit, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help stimulate a lively discussion.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u01d1 - Learning Components

- Recognize the need for policies on technical assets.

u01a1 - Implementing an Information Systems Security Policy

Overview

Information security policies and plans are increasingly important to the success of modern IT operations. Whether it is a nonprofit organization, a retail store, a financial enterprise or healthcare organization, threats to security are relevant and evident. Policies and plans help to outline and describe the security controls in place in order to improve an organization's security posture based on its risks, threats, and business needs.

In this assignment you will complete the lab, Implementing an Information Systems Security Policy and write security policies for Acceptable Use and Workstation Security.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. Use this Word template for your assignment submission.
- Read the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

- Open the Implementing an Information Systems Security Policy lab, found in this unit, and read the following:
    - Before You Begin.
    - Introduction.

Instructions

Part 1 – Complete All of Sections 1 and 2 of Implementing an Information Systems Security Policy Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration."
    - Part 1 Steps 14 and 31.
    - Part 2 Step 5.
    - Part 3 Step 41.
2. Complete "Section 2: Applied Learning."
    - Part 1 Steps 6 and 13.
    - Part 2 Step 4.
3. Based on the steps taken in the lab, explain how automated policy distribution (for example, Group Policy Objects, Puppet, et cetera.) can assist in the configuration and compliance of systems.

Part 2 - Security Planning: Acceptable Use and Workstation Security Policies

Create the following security policies for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create effective policies that represent modern systems assurance security practices and planning.

1. Acceptable Use (2–3 pages).
2. Workstation Security for a regulated healthcare environment (1–2 pages).

Consider the following scoring guide criteria as you complete your assignment:

- Write an Acceptable Use policy that is appropriate for the Course Security Scenario.
- Write a Workstation Security policy that is appropriate for the Course Security Scenario.
- Explain how automated policy distribution can assist in the configuration and compliance of systems.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources

Course Security Scenario

Assignment Template

u01v1 - Implementing an Information Systems Security Policy

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.

Unit 2 >> Malicious Attacks, Threats, and Vulnerabilities

Introduction

This unit discusses general infrastructure security issues, the use of intrusion detection systems, and the advantages and disadvantages related to each system. Infrastructure security relates primarily to viewing the

entirety of information assets as a comprehensive system. Security functions best when implemented in layers. Infrastructure security planning should address how these layers can be used to complement one another.

In this unit you will examine how vulnerabilities can negatively affect the security posture of an organization and also perform hands-on scans to see where a system may have vulnerabilities and risks that could be mitigated, transferred, avoided, or accepted.

Learning Activities

u02s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 3, "Malicious Attacks, Threats, and Vulnerabilities," pages 72–110.

Read the following on the Internet:

- United States Postal Service. (2017). Patch management process. Retrieved from https://about.usps.com/doing-business/it-policies-standards/Patch-Management-Process.htm
  - This is a real-world example of a patch management process and policy.
- Barth, B. (2018). The Top Cybersecurity Threats for 2017. Retrieved from https://www.scmagazine.com/the-top-cybersecurity-threats-for-2017/article/720097
  - This is an overview of the top cybersecurity threats in 2017.
- Breeden II, J. (2017). What is vulnerability management? Retrieved from https://www.csoonline.com/article/3238080/vulnerabilities/what-is-vulnerability-management-processes-and-software-for-prioritizing-threats.html
  - This is an article explaining the details of vulnerability management.

Skillsoft Resources

View the following Skillsoft video:

- Shannon, M. (n.d.). CompTIA Security+ SY0-501: Types of Malware [Video]. Skillsoft Ireland.(56 min.).

Optional Reading

- Beyond Trust. (2017). Sample vulnerability management policy Retrieved from https://www.beyondtrust.com/wp-content/uploads/wp-sample-vulnerability-management-policy.pdf?1446594949
  - This is a sample of a vulnerability management policy.

u02s1 - Learning Components

- Read the Course Security Scenario.
- Understand the importance of vulnerability management in organizations.
- View an example of vulnerability management strategy.
- Recognize the need for patch management in organizations.
- View an example of a patch management policy.
- Recognize the need for security scanning in organizations.
- Understand the uses of scanning software.

u02d1 - Vulnerability Management Project

Discuss the importance of vulnerability management and ongoing vulnerability management planning. Describe challenges from management and other IT professionals that a security professional might encounter in developing and implementing a vulnerability management plan.

Response Guidelines

Respond to at least two other learners' posts.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u02d1 - Learning Components

- Understand the importance of vulnerability management in organizations.

u02a1 - Performing a Vulnerability Assessment

Overview

There are many important mantras in the information security and assurance space, including, *we can't protect what we don't know we have*. One of the next steps after we know what we need to protect is to learn where we are vulnerable on those assets we need to protect. One of the common ways to do this is performing vulnerability assessments on our assets and developing strategies for managing the risk that result from those vulnerabilities.

In this assignment you complete the Performing a Vulnerability Assessment lab and write policies for Vulnerability and Patch Management.

Preparation

Do the following:

- Download the Assignment X Template. Use this Word template for your assignment submission.
- Open the Performing a Vulnerability Assessment lab found in this unit and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in Part 2.

Instructions

Part 1 - Complete All of Sections 1 and 2 of the Performing a Vulnerability Assessment Lab

Note: not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration."
    - Part 1 Steps 10, 16 and 20.
2. Complete "Section 2: Applied Learning."
    - Part 1 Steps 6, 11 and 15.
3. Based on the specific actions taken in the lab, compare and contrast the information received from Nessus and Nmap and indicate which you believe to be more valuable and why.

Part 2 - Security Planning: Vulnerability and Patch Management

Create the following security policies for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create effective policies that represent modern systems assurance security practices and planning.

1. Vulnerability Management (1 page).
2. Patch Management (1–2 pages).

Consider the following scoring guide criteria as you complete your assignment:

- Write a vulnerability management policy that is appropriate for the Course Security Scenario.
- Write an application Patch Management policy that is appropriate for the Course Security Scenario.
- Compare and contrast the information received from Nessus and Nmap.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources

Course Security Scenario
Assignment Template

u02v1 - Performing a Vulnerability Assessment

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.

Unit 3 >> The Drivers of the Information Security Business

Introduction

There are many axioms used in the information assurance and security profession, one emphasized in this unit is that a single security control will eventually fail. This is what makes layered security security defenses a very

important part of this concept, so that when a single control does indeed fail, there are other controls in place that will together help mitigate the risk of the failed control.

In this unit you will examine the concept of layered security and explore some of the layered controls that could be put in place for defense-in-depth coverage of security operations.

Learning Activities

u03s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 4, "The Drivers of the Information Security Business," pages 115–131.

Read the following on the Internet:

- Shenk, J. (2013). Layered security: why it works Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/layered-security-works-34805
    - This white paper covers the importance of layered security defenses.
- Masters, G. (2017). Shift in password strategy from NIST. Retrieved from https://www.scmagazine.com/shift-in-password-strategy-from-nist/article/663269
    - This article outlines the change in view of password complexity by NIST.
- Nakashima, E. (2018). FBI chief calls encryption a 'major public safety issue.' Retrieved from https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html?utm_term=.0c5896f7198f
    - This article talks about how encryption can be detrimental in certain instances.

Skillsoft Resources

View the following Skillsoft video:

- Skillsoft. (n.d.). CISM: Information Security Governance (Part 1) [Video]. Skillsoft Ireland. (2 hrs.).

Optional Reading

- Computer Security Incident Response Team. (n.d.). InfoSec password policy Retrieved from http://www.csirt.org/sample_policies/sans/Password_Policy.doc
    - This is a policy template for password management and construction.

u03s1 - Learning Components

- Understand the need for vulnerability management in organizations.
- Read the Course Security Scenario.
- View an example of how to handle vulnerabilities in organizations.
- Understand differing logging components that can exist in a technology environment.
- View an example of a logging standards policy.
- Determine the importance of disabling unneeded services.
- Recognize the need for hardening systems in an organization.

u03s2 - Kaltura Media (optional)

In preparation for creating the audio recordings required for this course, complete the following **only if you plan to use Kaltura for your presentation**:

- If you have not already done so, install your audio recording device on your computer, using the installation instructions from the manufacturer.
- Practice using the audio equipment to ensure the audio quality is sufficient.
- Refer to the Using Kaltura tutorial for directions on recording and uploading your recordings in the courseroom.

Note: If you require the use of assistive technology or alternative communication methods to participate in this activity, please contact Disability Services to request accommodations.

u03s2 - Learning Components

- Familiarity with presentation software.

u03d1 - Layered Defenses

Suppose you were tasked with creating a layered security approach for a remote workforce in a healthcare organization. Consider the three (3) most important layered controls you would consider implementing for this workforce, and indicate why you believe those controls to be the most important.

Response Guidelines

Comment on the posts of at least two other learners.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u03d1 - Learning Components

- View an example of how to handle vulnerabilities in organizations.

u03a1 - Eliminating Threats with a Layered Security Approach

Overview

There are many key concepts of information assurance and security, but one important fact to note is that eventually, over time, a single security control will eventually fail. This is what makes layered security defenses a very important part of this concept, so that when a single control does indeed fail, there are other controls in place that will together help mitigate the risk of the failed control.

In this assignment you will complete the Eliminating Threats With a Layered Security Approach lab and write policies for Password Management and Logging Standards.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. You will use this Word template for your assignment submission.
- Open Eliminating Threats with a Layered Security Approach, found in this unit, and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in Part 2.

Kaltura

For part 2 of this assignment, you may choose to create your presentation using Kaltura. To learn how to use Kaltura, refer to the Using Kaltura tutorial linked in the Resources. Note, you will submit this portion of the assignment separately from parts 1 and 2.

Note: If you require the use of assistive technology or alternative communication methods to participate in these activities, please contact Disability Services to request accommodations.

Instructions

Part 1 - Eliminating Threats With a Layered Security Approach Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration."
    - Part 1 Steps 18 and 27.
    - Part 2 Step 9.
    - Part 3 Steps 8 and 17.
2. Complete "Section 2: Applied Learning."
    - Part 1 Steps 6, 8 and 13.
    - Part 2 Step 5.
    - Part 3 Steps 6 and 8.
3. Based on the specific actions taken in the lab, interpret the importance of disabling unneeded services and the potential detriment if these efforts are not taken.

Part 2 - Security Planning: Password Management and Logging Standards Presentation

Consider the following policies using information found in the Course Security Scenario as context.

1. Password Management.
2. Logging Standards.

Create a 10–15 minute presentation (using a common presentation software of your choice) that describes Password Management **and** Logging Standards policies that you would recommend to stakeholders interested in organizational security for the company described in the Course Security Scenario. Your presentation must include audio narration with supporting visual depictions.

Consider the following scoring guide criteria as you complete your assignment:

- Create a password management policy that is appropriate for the Course Security Scenario.
- Create a logging standards policy that is appropriate for the Course Security Scenario.
- Interpret the importance of disabling unneeded services and the potential detriment if this is not done.
- Create a presentation that accurately communicates a security plan to stakeholders.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Submit part 3 in a separate file. If the file exceeds 15 Mb, please zip the file.

Course Resources
Assignment Template
Course Security Scenario

Disability Services

Using Kaltura [PDF]

u03v1 - Eliminating Threats with a Layered Security Approach

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.

Unit 4 >> Access Controls

Introduction

An important component of an effective security management program includes ensuring that users are well-trained and are given only the access that is necessary to accomplish their tasks. It is important for security professionals to explore the technical controls that can be applied to support these guidelines, and consider the procedures and overall framework that allows these guidelines to be implemented comprehensively and at an enterprise level.

In this unit you will explore how Active Directory can be used in Windows environments to implement suitable and comprehensive access control policies, to ensure the confidentiality, integrity, and availability of systems and data.

Learning Activities

u04s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 5, "Information Systems Security," pages 137–167.

Read the following on the Internet:

- SSI Staff. (2018). HID global forecasts 5 top access control trends for 2018. Retrieved from https://www.securitysales.com/access/hid-global-access-control-trends-2018
    - This article discusses trends in access control for 2018.

Skillsoft Resources

View the following Skillsoft video:

- Skillsoft. (n.d.). Systems Security Certified Practitioner: Access Controls [Video]. Skillsoft Ireland. (1 hr. 3 min.).

Optional Reading

- South Carolina Department of Administration. (2014). Information security policy – access control. Retrieved from http://www.admin.sc.gov/files/InformationSecurityPolicy-AccessControl.docx
    - This is a real-world example of a logical access control policy.

u04s1 - Learning Components

- Read the Course Security Scenario.
- Understand the specific components of an access control policy.
- Determine the critical components of a physical access control policy.
- View an example of a physical access control policy.
- Recognize the need for elevated accounts and their effect on security.
- Understand the relevance of administrator/elevated accounts.

u04d1 - Access Controls in the Cloud

A common approach many organizations are taking in relation to file storage and collaboration is using cloud-based offerings such as Box, Dropbox, Google Drive, and others. However, with the increased collaboration and scalability there are security challenges that result as this shift progresses.

- Indicate what you believe to be the two (2) biggest challenges in implementing access controls and security in a cloud-based storage application? Explain.
- What compensating controls might you consider implementing to reduce risk and potential data loss presented by these challenges. Why are they appropriate?

Response Guidelines

Respond to at least two other learners' posts.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u04d1 - Learning Components

- Understand the specific components of an access control policy.

u04a1 - Enabling Windows Active Directory and User Access Controls

Overview

It is critical for an organization to protect its information resources in a compliant and assured manner. One of the first steps in this process is understanding what you need to protect and then you can determine who needs what access to particular resources. Using Active Directory and applying access controls to resources in that type of environment is one common way to secure these resources.

In this assignment you complete the Enabling Windows Active Directory and User Access Controls lab and write policies for Logical and Physical Access Control.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. Use this Word template for your assignment submission.

- Open the Enabling Windows Active Directory and User Access Controls lab, found in this unit, and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

Instructions

Part 1 - Complete All of Sections 1 and 2 of the Enabling Windows Active Directory and User Access Controls Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration."
    - Part 1 Step 34.
    - Part 4 Steps 17 and 13.
2. Complete "Section 2: Applied Learning."
    - Part 1 Step 9.
    - Part 2 Step 17.
    - Part 4 Step 7 and 11.
3. Based on your experience in the lab, justify an instance where an administrator may need to login to a server or workstation with an account different from their standard operating account.

Part 2 - Security Planning: Logical and Physical Access Control

Create the following security policies for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create effective policies that represent modern systems assurance security practices and planning.

1. Logical Access Control (2–3 pages).
2. Physical Access Control (2–3 pages).

Consider the following scoring guide criteria as you complete your assignment:

- Write a Logical Access Control policy that is appropriate for the Course Security Scenario.
- Write a Physical Access Control policy for HIPAA compliance that is appropriate for the Course Security Scenario.
- Justify an instance where an administrator may need to login to a server or workstation with an account different from their standard operating account.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources
Assignment Template
Course Security Scenario

u04v1 - Enabling Windows Active Directory and User Access 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.

Unit 5 >> Security Operations and Administration

Introduction

Designing, implementing, and maintaining a secure network involves hardening all of the individual devices by performing tasks that include securing any default passwords or administrator accounts, patching vulnerabilities in a timely manner, and closing off any unnecessary ports and services.

This unit explores techniques for hardening operating systems and applications and the vulnerabilities that result from not doing so, using tools such Group Policy Objects and the Microsoft Baseline Security Analyzer, which in tandem can provide security professionals extremely useful data for securing systems and data.

Learning Activities

u05s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 6, "Information Systems Security," pages 182–213.

Read the following on the Internet:

- AICPA. (n.d.). Segregation of duties. Retrieved from https://www.aicpa.org/interestareas/informationtechnology/resources/auditing/internalcontrol/value-strategy-through-segregation-of-duties.html
    - This provides an example of components to include in a separation of duties policy.
- O'Donovan, C. (2015). SecDevOps: embracing the speed of DevOps and continuous delivery in a secure environment. Retrieved from: https://securityintelligence.com/secdevops-embracing-the-speed-of-devops-and-continuous-delivery-in-a-secure-environment
    - This article explains the securing of DevOps.
- Tischart, J. (2016). DevOpsSec, SecDevOps, DevSecOps: What's in a name? Retrieved from: https://www.csoonline.com/article/3132078/security/devopssec-secdevops-devsecops-whats-in-a-name.html
    - This article covers the alignment of SecOps and DevOps.
- O'Donovan, C. (2017). SecOps revisited: the challenge of DevOps for security. Retrieved from: https://securityintelligence.com/secops-revisited-the-challenge-of-devops-for-security
    - This article explains the securing of DevOps.

Skillsoft Resources

View the following Skillsoft videos:

- Skillsoft. (n.d.). CISSP: Security Operations Part 1 [Video]. Skillsoft Ireland. (2 hrs. 26 min.).

- Hendry, B. (n.d.). DevOps Fundamentals: Providing Security [Video]. Skillsoft Ireland. (4 min.).

Optional Reading

- MyPM. (n.d.). Change management plan. Retrieved from http://7629-presscdn-0-90.pagely.netdna-cdn.com/wp-content/uploads/2015/02/Change-Management-Plan.docx
    - This is a template for developing a change management plan.

u05s1 - Learning Components

- Read the Course Security Scenario.
- Determine the critical components of a Separation of Duties policy.
- View an example of a Separation of Duties policy.
- Recognize the key components of a change management policy.
- View an example of a change control management policy.
- Recognize the need for security scanning in organizations.
- Understand the usefulness of group policy objects in organizations.

u05d1 - SecDevOps

Over the past 5–10 years there has been a shift in product and service development to use more agile methodologies to provide more continuous delivery.

Read the article SecDevOps: Putting Security at the Heart of DevOps.

Comment on at least two (2) security concerns with a DevOps model and how these concerns can be alleviated with a strong implementation of SecDevOps considerations.

Response Guidelines

Respond to at least two other learners' posts.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u05d1 - Learning Components

- Determine the critical components of a Separation of Duties policy.

u05a1 - Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control

Overview

As we have learned in previous labs, Group Policy Objects (GPOs) can be powerful assets for security administrators to ensure technical policies are forced on objects to achieve compliance. Additionally, the use of the Microsoft Baseline Security Analyzer can help determine needed secure standards and provide models that can be implemented using GPOs in a Microsoft environment.

In this assignment you will complete the Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control lab and write policies for Separation of Duties and Change Control Management.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. You will use this Word template for your assignment submission.
- Open the Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control lab, found in this unit. and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

Instructions

Part 1 - Complete All of Sections 1 and 2 of Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration."
    - Part 1 Step 19.
    - Part 3 Step 10.
2. Complete "Section 2: Applied Learning."
    - Part 1 Steps 6.
    - Part 2 Step 10.
    - Part 3 Step 3.
3. Based on the tasks performed in the lab, explain how GPOs and the MBSA can work together to provide a better overall security posture in a Windows environment.

Part 2 - Security Planning: Separation of Duties and Change Control Management

Create the following security policies for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create effective policies that represent modern systems assurance security practices and planning.

1. Separation of Duties (1–2 pages).
2. Change Control Management (2–3 pages).

Consider the following scoring guide criteria as you complete your assignment:

- Write a Separation of Duties policy that is appropriate for the Course Security Scenario.
- Write a Change Control Management policy that is appropriate for the Course Security Scenario.
- Explain how GPOs and the MBSA can work together to provide a better overall security posture in a Windows environment.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources
Course Security Scenario
Assignment Template

u05v1 - Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control

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.

Unit 6 >> Auditing, Testing, and Monitoring

Introduction

Auditing, testing, and monitoring are staples in today's information technology landscape. Testing is needed to ensure our products (and the products of others we use) are secure in our specific environments. Auditing is needed so that we own the governance needed to ensure ongoing, continuous security and compliance. Monitoring is needed to ensure that our operational controls are in place to detect, act, and react as needed.

In this unit you will use technical controls to explore the need for monitoring, including network packet capture and analysis using current tools and techniques. These controls are critical to network security operations and can provide security personnel with critical data in order to in order form a proper response.

Learning Activities

u06s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 7, "Information Systems Security," pages 217–249.

Read the following on the Internet:

- Cloud.gov. (n.d.). Continuous monitoring strategy. Retrieved from https://cloud.gov/docs/ops/continuous-monitoring
  - This provides guidance for creating a security monitoring strategy.
- UAB. (2016). HIPAA core policy: Information systems and network access. Retrieved from http://www.uab.edu/policies/content/Pages/UAB-AD-POL-0000724.aspx
  - This is a real-world healthcare example of an access approval policy.

- Kilpatrick, I. (n.d.). Security information and event management (SIEM) systems streamline compliance. Retrieved from http://www.computerweekly.com/tip/Security-information-and-event-management-SIEM-systems-streamline-compliance
    - This article explains the benefits of SIEM for security and compliance.

Skillsoft Resources

View the following Skillsoft video:

- Skillsoft. (n.d.). CISSP: Security Assessment and Testing [Video]. Skillsoft Ireland. (1 hr. 45 min.).

u06s1 - Learning Components

- Read the Course Security Scenario.
- Identify the key components of a monitoring policy.
- Familiarity with presentation software.
- Recognize the need for access request approvals and the effect on a security posture.
- View an example of an access request approval policy.
- Recognize the benefits of packet capture and analysis.
- Recognize the use of scanning tools in a secure environment.
- View an example of a business continuity plan.
- Understand the need for incident response efforts in organizations.
- View an example of an incident response procedure.
- Understand the uses of NFS in a Windows environment.
- Recognize technical components and effects on business continuity.
- Recognize the need for business continuity efforts in organizations.

u06d1 - Auditing and Monitoring

Auditing and monitoring are key components of any information security program. One of the most helpful solutions that organizations use in this space is SIEM (security information and event management) systems. An article referencing SIEM can be found in this unit's study.

Explain in your own words the benefits of a SIEM system and how you believe these products can assist in the overall compliance of organizations.

Response Guidelines

Comment on the posts of at least two other learners.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u06d1 - Learning Components

- Identify the key components of a monitoring policy.

u06a1 - Performing Packet Capture and Traffic Analysis

Overview

There are times when the inexplicable happens and as an administrator you are not sure what is happening. When these situations arise, it is valuable to have tools, such as packet capture and analysis tools, at your disposal so that you can conduct an efficient analysis. These types of tools can also come at a cost due to the type of data, potentially confidential data, that is captured. Additionally, monitoring and access approvals are key components to ensure data capture activities occur in a compliant manner.

In this assignment you will complete the Performing Packet Capture and Traffic Analysis lab and write policies for Monitoring and Access Request Approvals.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. Use this Word template for your assignment submission.
- Open the Performing Packet Capture and Traffic Analysis lab, found in this unit, and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

Kaltura

For part 2 of this assignment, you may choose to create your presentation using Kaltura. To learn how to use Kaltura, refer to the Using Kaltura tutorial found in the Resources. Note, you will submit this portion of the assignment separately from parts 1 and 2.

Note: If you require the use of assistive technology or alternative communication methods to participate in these activities, please contact Disability Services to request accommodations.

Instructions

Part 1 - Complete All of Sections 1 and 2 of the Performing Packet Capture and Traffic Analysis Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration:"
    - Part 1 Step 43, 53.
    - Part 2 Step 18.
    - Part 3 Step 11.
2. Complete "Section 2: Applied Learning:"
    - Part 1 Step 23, 30.
    - Part 2 Step 18.
    - Part 3 Step 5.
3. Based on the data collected in the lab, compare and contrast the uses of NetWitness Investigator and Wireshark. Include a discussion of the value of the data collected for each.

Part 2 - Security Planning: Monitoring and Access Request Approvals Presentation

Write the following using information found in the Course Security Scenario as context.

1. Monitoring (1 page).
2. Monitoring (1–2 pages).

Create a 10–15 minute presentation (using a common presentation software of your choice) that describes Monitoring **and** Access Request Approvals policies that you would recommend to stakeholders interested in organizational security for the company described in the Course Security Scenario. Your presentation must include audio narration with supporting visual depictions.

Consider the following scoring guide criteria as you complete your assignment:

- Create a monitoring policy that is appropriate for the Course Security Scenario.
- Create an access request approvals policy that is appropriate for the Course Security Scenario.
- Compare and contrast the uses of NetWitness Investigator and Wireshark and the value of the data collected.
- Create a presentation that accurately communicates a security plan to stakeholders.

Additional Instructions

Place your well-labeled written work in the Assessment X Template and submit it.

Submit part 2 in a separate file. If the file exceeds 15 MB, please zip the file.

Course Resources
Disability Services

Course Security Scenario
Assignment Template
Using Kaltura [PDF]

u06v1 - Performing Packet Capture and Traffic Analysis

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.

Unit 7 >> Risk, Response, and Recovery

Introduction

Risk, response, and recovery are key to organizations with today's ever-changing threat landscape and the increased demand for high availability. Whether it be from a power outage, attack, or natural disaster,

organizations are incentivized to ensure that they have proper policies, procedures, and plans in order to continue business operations regardless of what challenges are faced.

In this unit you will explore the need for business continuity planning and operations in organization, as well as how an organization might consider responding to incidents, including those mentioned above.

Learning Activities

u07s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 8, "Risk, Response, and Recovery," pages 252–286.

Read the following on the Internet:

- Ready.gov. (n.d.). Business continuity plan. Retrieved from https://www.ready.gov/business/implementation/continuity.
    - This provides guidance on creating a business continuity plan.
- Giffin, R. (2015). What you need to do: Cloud computing and business continuity. Retrieved from https://perspectives.avalution.com/2015/what-you-need-to-know-cloud-computing-and-business-continuity
    - This article explains some concerns and strategies for business continuity in the cloud.
- California Hospital Association. (2016). Hospital business continuity templates: Facility-wide BCP template. Retrieved from https://www.calhospitalprepare.org/sites/main/files/file-attachments/facility-wide_bcp_template.docx
    - This is a template for a healthcare business continuity plan.

Skillsoft Resources

View the following Skillsoft videos:

- Skillsoft. (n.d.). CISSP 2013 Domain: Business Continuity and Disaster Recovery Planning [Video]. Skillsoft Ireland. (1 hr. 30 min.).
- Skillsoft. (n.d.). CompTIA Security+ SY0-401: Continuity, Disaster Recovery, and Computer Forensics [Video]. Skillsoft Ireland. (1 hr. 55 min.).

Optional Reading

- California Department of Technology. (n.d.). Incident response plan example. Retrieved from https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc

- This is an example of a real-world incident response plan.

u07s1 - Learning Components

- Read the Course Security Scenario.
- Recognize the need for policies on technical assets.
- Understand the role of an acceptable use policy within an organization.
- View an example of an acceptable use policy.
- Understand the importance of workstation security.
- View an example of a workstation security policy.
- Understand the need for automated policy distribution in organizations.

u07d1 - SaaS Products and Services

Cloud offerings and software-as-a-service (SaaS) solutions have changed the way organizations operate over the past number of years; this is also very relevant for the continuity efforts of organizations in all industries.

Describe how cloud and SaaS products and services impact the business continuity efforts of organizations. Discuss what you believe to be the two (2) most impactful ways in which these offerings aid business continuity efforts.

Response Guidelines

Comment on the posts of at least two other learners.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u07d1 - Learning Components

- Consider the key components of a business continuity plan.

u07a1 - Implementing a Business Continuity Plan

Overview

The ever-growing reliance that organizations have on technology comes with a need for business continuity planning. These plans help to ensure that, in periods of disruption or outage, the business has the policies and procedures needed to resume operations as quickly as possible, while minimizing the overall disruption. Business continuity efforts should be closely aligned with incident response plans that outline the needed processes for continuing operations during and after an incident occurs.

In this assignment you will complete the Implementing a Business Continuity Plan lab and write plans for Business Continuity and Incident Response.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. Use this Word template for your assignment submission.
- Open the Implementing a Business Continuity Plan, found in this unit, and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

Instructions

Part 1 - Complete All of Sections 1 and 2 of the Implementing a Business Continuity Plan Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration:"
    - Part 2 Step 18.
    - Part 3 Step 28.
    - Part 4 Steps 5, 10 and 19.
2. Complete "Section 2: Applied Learning:"
    - Part 2 Step 4.
    - Part 3 Step 18.
    - Part 4 Steps 4 and 11.
3. Based upon the steps taken in the lab, explain how configuring websites to use a common NFS share could strengthen business continuity efforts.
4. Explain how this lab demonstrates the importance of business continuity efforts in organizations.

Part 2 - Security Planning: Business Continuity Planning and Incident Response Procedures

Create the following security policies for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create effective policies that represent modern systems assurance security practices and planning.

1. Business Continuity Planning (2–4 pages).
2. Incident Response Procedures (2–3 pages).

Consider the following scoring guide criteria as you complete your assignment:

- Write a business continuity plan that is appropriate for the Course Security Scenario.
- Write an incident response procedure policy that is appropriate for the Course Security Scenario.
- Explain how configuring Websites to use a common NFS share could strengthen business continuity efforts.
- Explain how the lab demonstrates the importance of business continuity efforts in organizations.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources
Assignment Template
Course Security Scenario

u07v1 - Implementing a Business Continuity Plan

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.

Unit 8 >> Cryptography

Introduction

Encryption technologies are staples in many organizations of today's computing world. From secure websites that are accessed using these technologies, to database encryption of personal information stored on a business' server, to secure communications between businesses, customers, governments and more. Encryption is here to stay and our reliance on it is poised to grow.

In this unit, you will explore the various ways encryption is used within the context of operating system security and how it can be used for the overall confidentiality of an organization's data. You will also develop a strategy for integrating encryption into your overall security plan.

Learning Activities

u08s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 9, "Cryptography," pages 289–323.

Read the following on the Internet:

- NHS Digital. (2017). Encryption: example policy. Retrieved from https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/encryption-guidance-for-health-and-care-organisations/encryption-example-policy
  - This is a template for an encryption policy.
- Snell, E. (2015). Breaking down HIPAA: health data encryption requirements. Retrieved from https://healthitsecurity.com/news/breaking-down-hipaa-health-data-encryption-requirements
  - This article covers encryption specifics with HIPAA.
- Affinity Health System. (n.d.). Remote access request policy Retrieved from http://www.affinityhealth.org/OffNav/Remote-Access-Request-Policy.htm

- This is a real-world healthcare example of a remote access policy.

Skillsoft Resources

View the following Skillsoft videos:

- Skillsoft. (n.d.). Microsoft Windows Server 2012 R2 - Administration: File Services and Encryption [Video]. Skillsoft Ireland. (2 hrs. 30 min.).
- Murphy, M. (n.d.). Implementing Disk Encryption [Video]. Skillsoft Ireland. (1 hr. 4 min.).

u08s1 - Learning Components

- Read the Course Security Scenario.
- Understand the need for encryption technologies in the healthcare industry.
- View an example of an encryption usage policy.
- Recognize the key components of a remote access policy.
- View an example of a remote access policy.
- Recognize the need for encryption to secure data.
- Understand the components of asymmetric encryption.

u08d1 - Encryption Technologies

Encryption technologies are commonplace in today's technology world and in many cases are a necessity. While these technologies can surely assist organizations in protecting their valuable assets, they can also be used for malicious activities.

Indicate at least one (1) inventive way in which you believe organizations are using encryption technologies in the healthcare industry to protect their assets, and at least one (1) way in which you believe attackers can use encryption technologies to carry out malicious activities.

Response Guidelines

Comment on the posts of at least two other learners.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u08d1 - Learning Components

- Understand the need for encryption technologies in the healthcare industry.

u08a1 - Using Encryption to Enhance Confidentiality

Overview

Organizations are finding more and more reasons to invest in and use encryption technologies to protect confidential information. Additionally, the need for encryption technologies is critical to many compliance efforts with certain laws and regulations to which many industries are bound. Encrypting traffic, systems, and data at rest are key components to an overall encryption strategy.

In this assignment you will complete the Using Encryption to Enhance Confidentiality lab and write policies for Encryption Usage and Remote Access.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. You will use this Word template for your assignment submission.
- Open the Using Encryption to Enhance Confidentiality lab, found in this unit, and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

Instructions

Part 1 - Complete All of Sections 1 and 2 of the Using Encryption to Enhance Confidentiality Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete “"Section 1: Hands-on Demonstration:"
    - Part 1 Steps 11 and 17.
    - Part 4 Step 22.
2. Complete "Section 2: Applied Learning:"
    - Part 1 Steps 5 and 9.
    - Part 2 Step 4.
    - Part 3 Step 5.
3. Based on the steps taken in the lab, explain why both public and private keys are needed in an asymmetric key pair.

Part 2 - Security Planning: Encryption Usage and Remote Access

Create the following security policies for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create effective policies that represent modern systems assurance security practices and planning.

1. Encryption Usage in a regulated healthcare environment (1–2 pages).
2. Remote Access (1 page).

Consider the following scoring guide criteria as you complete your assignment:

- Write an encryption usage policy that is appropriate for the Course Security Scenario.
- Write a remote access policy that is appropriate for the Course Security Scenario.
- Explain why both public and private keys are needed in an asymmetric key pair.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources
Course Security Scenario
Assignment Template

u08v1 - Using Encryption to Enhance Confidentiality

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.

Unit 9 >> Networks and Telecommunications

Introduction

While covering the various aspects and components of organizational security, you have seen that layered controls can improve the security posture of an organization. The use of encryption to protect the security and privacy of information collected and stored on the network occurs using a range of solutions and many network devices and components.

In this unit, you will explore the various ways to secure networks and the many controls that can be implemented to enhance an organization's secure operations with a network security and devices plan.

Learning Activities

u09s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 10, "Networks and Telecommunications," pages 327–351.

Read the following on the Internet:

- SANS Consensus Policy Resource Community. (2014). Wireless communication policy. Retrieved from https://www.sans.org/security-resources/policies/network-security/pdf/wireless-communication-policy
  - This is a template for a network device security policy.
- National Institute of Standards and Technology. (n.d.). Intrusion Detection and Prevention Systems. Retrieved from http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901146
  - This is an overview of intrusion detection and prevention systems.

Skillsoft Resources

View the following Skillsoft video:

- Skillsoft. (n.d.). CISSP: Communication & Network Security Design [Video]. Skillsoft Ireland. (2 hrs.).

u09s1 - Learning Components

- Read the Course Security Scenario.
- Understand the need for securing network devices in an organization.
- View an example of a network device security policy.
- Recognize the need for intrusion detection processes in an organization.
- View specifics of intrusion detection processes.
- Recognize some key components of reconnaissance efforts.
- Understand the key uses of the Zenmap product.

u09d1 - Layering Defenses

In today's world, there are still some organizations that believe sufficient network security protection begins and ends with a firewall. With the concept of layered defenses in mind, provide at least three (3) layered network security defenses in addition to a firewall that organizations could and should consider implementing. Additionally, of the three selected, indicate which you believe to be the most important and why.

Response Guidelines

Comment on the posts of at least two other learners.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u09d1 - Learning Components

- Understand the need for securing network devices in an organization.

u09a1 - Performing Reconnaissance and Probing Using Common Tools

Overview

One of the key components of an information security program is ensuring that potential attacks and anomalous activity are prevented and detected in a timely fashion. This key action is accomplished using intrusion detection and prevention systems (IDS/IPS). Additionally, in order to increase security governance and posture, many organizations also perform penetration and ethical hacking testing, which can be useful in detecting security vulnerabilities before others.

In this assignment you will complete the Performing Reconnaissance and Probing Using Common Tools lab and write policies for Network Device Security and Intrusion Detection.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. Use this Word template for your assignment submission.
- Open the Performing Reconnaissance and Probing Using Common Tools lab, found in this unit, and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

Instructions

Part 1 - Complete All of Sections 1 and 2 of the Performing Reconnaissance and Probing Using Common Tools Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration:"
    - Part 1 Steps 18 and 25.
    - Part 3 Step 17.
2. Complete "Section 2: Applied Learning:"
    - Part 1 Steps 8, 14, 23 and 40.
    - Part 2 Step 14.
    - Part 3 Step 5 and 7.
3. Based on the actions taken in the lab, explain in detail the information that was gained in using Zenmap for reconnaissance efforts.

Part 2 - Create a Policy for Network Architecture

Create the following security policies for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create effective policies that represent modern systems assurance security practices and planning.

1. Network Device Security (2–3 pages).
2. Intrusion Detection (1–2 pages).

Consider the following scoring guide criteria as you complete your assignment:

- Write a network device security policy that is appropriate for the Course Security Scenario.
- Write an intrusion detection process that is appropriate for the Course Security Scenario.
- Explain the information that is gained in using Zenmap for reconnaissance efforts.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources
Assignment Template
Course Security Scenario

u09v1 - Performing Reconnaissance and Probing Using Common Tools

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.

Unit 10 >> Malicious Code and Activity

Introduction

Understanding potential threats to information assets is necessary in order to identify both the level of risk and the potential controls that can be used to mitigate those threats. The range of potential threats to information assets is wide and varied, covering everything from locks and keys to account management, business continuity, and the securing of data through access controls and backup procedures.

In this unit you will explore some of the protections that might be implemented to protect from a multitude of threats and contribute to an organization's overall information security program.

Learning Activities

u10s1 - Studies

Readings

Read the following in your *Fundamentals of Information Systems Security* text:

- Chapter 11, "Malicious Code and Activity," pages 355–398.

Read the following on the Internet:

- OWASP. (2016). Testing guide introduction. Retrieved from https://www.owasp.org/index.php/Testing_Guide_Introduction
  - This is a road map for security testing applications.
- OWASP. (2017). Web application security testing cheat sheet. Retrieved from https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet
  - This provides useful information for Web application security testing.
- SANS Consensus Policy Resource Community. (2014). Web application security policy. Retrieved from https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy
  - This is a template for a Web application security and testing policy.

Skillsoft Resources

View the following Skillsoft videos:

- Skillsoft. (n.d.). Certified Ethical Hacker (CEH): Hacking Web Applications [Video]. Skillsoft Ireland. (1 hr. 30 min.).
- Lachance, D. (n.d.). Vulnerabilities and Exploits [Video]. Skillsoft Ireland. (59 min.).
- Lachance, D. (n.d.). Systems Security Certified Practitioner: Systems and Application Security [Video]. Skillsoft Ireland. (2 hrs. 6 min.).

u10s1 - Learning Components

- Read the Course Security Scenario.
- Recognize the need for policies on technical assets.
- Understand the role of an acceptable use policy within an organization.
- View an example of an acceptable use policy.
- Understand the importance of workstation security.
- View an example of a workstation security policy.
- Understand the need for automated policy distribution in organizations.
- Understand the need for application and security testing.
- View an example of an application security and testing plan.
- Recognize the need for protections from malicious attacks.

u10d1 - Database Protection

Since databases can be key targets for attackers, database protection is an extremely critical component of an information security program. Discuss a common attack that may be used to compromise a database system, and at least one (1) protective measure that might be taken to prevent that attack.

Response Guidelines

Comment on the posts of at least two other learners.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u10d1 - Learning Components

- Understand the key components of Cross-Site Scripting and SQL Injection attacks.

u10a1 - Performing a Website and Database Attack by Exploiting Identified Vulnerabilities

Overview

As the reliance on software-as-a-service (SaaS) providers increases in organizations, it is becoming more and more important for those SaaS providers to create secure products and services. One process that can help in these efforts is to competently secure and test applications with security in mind. Additionally, it is also relevant for security testers to understand certain hacking techniques that could be used by hackers in order to ensure products and services are not prone to certain attacks, such as cross-site scripting and SQL injection.

In this assignment you will complete the Performing a Website and Database Attack by Exploiting Identified Vulnerabilities lab and write a policy for Application Security and Testing.

Preparation

Do the following using items found in the Resources:

- Download the Assignment X Template. You will use this Word template for your assignment submission. *Please ignore the [Item 2.2] portion of the template as it is not required for this assignment.*
- Open the Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities lab, found in this unit, and read the introduction.
- Review the Course Security Scenario document found in the Resources for context when writing your security policies in part 2.

Instructions

Part 1 - Complete All of Sections 1 and 2 of the Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities Lab

Note: Not all sections mentioned in the lab's directions are required for this assignment.

Do the following:

1. Complete "Section 1: Hands-on Demonstration:"
    - Part 1 Step 8, 11.
    - Part 2 Step 18.
2. Complete "Section 2: Applied Learning:"
    - Part 1 Step 5, 8.
    - Part 2 Step 12.
3. Based on the specific actions taken in the lab, compare and contrast Cross-Site Scripting and SQL Injection attacks, including with the effort needed and value of each attack.

Part 2 - Security Planning: Application Security and Testing

Create an application Security and Testing policy for the company described in the Course Security Scenario. State any assumptions that you make, or details that might add depth, texture, or provide a foundation for your policies. Your goal is to create an effective policy that represent modern systems assurance security practices and planning.

Consider the following scoring guide criteria as you complete your assignment:

- Write an application security and testing plan that is appropriate for the Course Security Scenario.
- Compare and contrast Cross-Site Scripting and SQL Injection attacks.

Additional Instructions

Place your well-labeled written work from parts 1 and 2 in the Assignment X Template and submit it.

Course Resources
Assignment Template
Course Security Scenario

u10v1 - Virtual Resource: Hands-on Labs

Click the linked title in the heading above to access and complete the following tasks related to **CompTIA Security+** certification-related content and activities, provided via the Virtual Resource Portal. Refer to the guides found in the Resources for support.

Practice Labs

Within the **CompTIA Security+ Certification** bundle, click the **Practice Labs** option to access the lab of your choice.

Practice Exams

You are highly encouraged to complete the following practice exams to test your knowledge. These activities will also help you prepare to qualify for an exam voucher. See the IT Industry Certifications page for qualifying criteria details.

Within the **CompTIA Security+ Certification** bundle, click the **Practice Exams** option to access corresponding practice activities. A screen appears with three options. In this unit, it is recommended that you

complete the following activities:

- Use the **Optimize Exam Experience** option to complete all exam questions related to the following:
  - **Threats and Vulnerabilities.**
  - ***Access Control and Identity Management.***
  - ***Application, Data, and Host Security.***
  - ***Cryptography.***
  - ***Network Security.***

Note that you can choose the **Grade Item** option to receive immediate feedback on your responses.

- Use the **TranscenderFlash** option to complete related flashcards.

Course Resources

Virtual Resource: Hands-on Labs

u10v2 - Performing a Website 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.