Preview: IT4070 : Cyber Defense and Countermeasures

Syllabus

Course Overview

This course focuses on the basics of developing a secure information technology network infrastructure by exploring and employing defense in-depth structures such as policy, risk, exposures, countermeasures, network configuration, law, and controls. You will examine security issues associated with VPNs, intrusion detection, firewalls, and other network infrastructure components and processes. Ultimately, you have the opportunity to apply your knowledge to assess network components and recommend solutions to mitigate exposures in assignments, discussions, and virtual labs.

The course requires you to create a more secure network infrastructure based on the Anchor Hospital Scenario document. There is no cumulative deliverable for the course, but you will complete a series of assignments that covers a variety of network security aspects that include:

1. Network weakness and threat identification.
2. Firewalls.
3. Physical security.
4. Cloud security.
5. Intrusion detection.
6. VPN solutions.
7. Incidence response and reporting.
8. Security policy.
9. Encryption defense.
10. Risk assessment and mitigation.

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 assignments.

Disability Services

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

Course Competencies

(Read Only)

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

1. Apply network security solutions.
2. Apply secure remote access, email, and data transmission solutions.
3. Apply cyber security countermeasures.
4. Explain how risk analysis and information security policy support a secure infrastructure.
5. Analyze legal and ethical considerations associated with developing a secure network.
6. Communicate effectively and professionally.

Course Prerequisites

Prerequisite(s): IT3355, 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.

Book

Capella University (Ed.). (2019). *IT4070: Cyber defense and countermeasures* [Custom online lab bundle]. Burlington, MA: Jones & Bartlett. ISBN: 9781284456639.

Easttom, C. (2018). *Network defense and countermeasures: Principles and practices* (3rd ed.). Indianapolis, IN: Pearson. ISBN: 9780789759962.

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.

- Anandamurugan, S., Priyaa, T., & Arvind Babu, M. C. (2017). *Cloud computing: An innovative technology for Linux and Android platforms.* Skillsoft Ireland.
- Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials.* Skillsoft Ireland.
- Clarke, G. E. (2018). *CompTIA network+ certification study guide* (7th ed.). Skillsoft Ireland.
- Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA Security+ and beyond* (fifth ed.) (Exam SY0-501). Skillsoft Ireland.
- Gibson, D. (2018). *SSCP Systems security certified practitioner all-in-one exam guide* (third ed.). Skillsoft Ireland.
- Gupta, B. B., Agrawal, D. P., & Wang, H. (Eds.). (2019). *Computer and cyber security: Principles, algorithm, application, and perspectives.* Skillsoft Ireland.
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
- Hu, H., Ahn, G.-J., & Kulkarni, K. (2010). FAME: A firewall anomaly management environment. In *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration* (pp. 17–26). New York, NY: ACM.
- Pathan, A. K. (Ed.). (2014). *The state of the art in intrusion prevention and detection.* Skillsoft Ireland.
- Shannon, M. (2018). *CompTIA Security+ SY0-501: Components supporting organizational security* [Tutorial]. Skillsoft.
- Skillsoft. (n.d.). *CompTIA Cloud+ CV0-001: Cloud security* [Tutorial].
- Skillsoft. (n.d.). *CompTIA Cloud+ CV0-002: Security technologies and automation techniques* [Tutorial]. null
- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
- Skillsoft. (n.d.). *Cybersecurity 101: Auditing and incident response* [Tutorial].

- Skillsoft. (n.d.). *Cybersecurity 101: Session & risk management: Asset, threats, and vulnerabilities* [Tutorial].
- Skillsoft. (n.d.). *Moving business services into the cloud* [Tutorial]. null
- Skillsoft. (n.d.). *Security fundamentals: Firewalls* [Tutorial].
- Skillsoft. (n.d.). *SSCP domain: Risk, response, and recovery* [Tutorial].
- Skillsoft. (n.d.). *SSCP domain: Security operations and administration part 1* [Tutorial].
- Vacca, J. R. (2017). *Security in the private cloud.* Skillsoft Ireland.
- Willcocks, L., Venters, W., & Whitley, E. A. (2014). *Moving to the cloud corporation: How to face the challenges and harness the potential of cloud computing.* 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.

- Covington, R. C. (2015, Jun 23). Physical security: The overlooked domain [Blog post]. Retrieved from https://www.csoonline.com/article/2939322/physical-security-the-overlooked-domain.html
- Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2008). Guide to SSL VPNs: Recommendations of the National Institutes of Standards and Technology [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- Microsoft. (n.d.). Create a network diagram. Retrieved from https://support.office.com/en-us/article/video-create-a-network-diagram-a2360cd9-5c9d-4839-b4f6-17b485e02262
- National Institute of Standards and Technology (NIST). (2012). NIST special publication 800-30 r1: Guide for conducting risk assessments [PDF]. Available from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- National Institute of Standards and Technology. (n.d.). Computer security resource center. Retrieved from https://csrc.nist.gov/
- National Institutes of Standards and Technology (NIST). (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- Rose, S., Nightingale, J. S., Garfinkel, S. L., & Chandramouli, R. (2019). NIST special publication 800-177 revision 1: Trustworthy email [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
- Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy: Recommendations of the National Institute of Standards and Technology [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf
- Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D. I. (2008). An introductory resource guide for implementing the Health Insurance Portability Act (HIPAA) security rule [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

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.

- Microsoft. (n.d.). Memos. Retrieved from https://templates.office.com/en-us/Memos

Unit 1 >> Introduction to Network Security Defense and Countermeasures

Introduction

In this unit you:

- Discuss common network attacks.
- Diagram the Anchor Hospital network and identify its components and vulnerabilities.

Understanding a network infrastructure helps security professionals identify and prioritize potential threats, vulnerabilities, and risks. Unit 1 introduces some attacks that could be launched against a network. The following terms are discussed in this unit:

***Network defense*:** The act of defending against or resisting a network attack, largely considered to be preventative. Examples include:

- Firewalls.
- Intrusion Detection Systems (IDS).
- Virtual Private Networks (VPNs).

***Network countermeasure*:** A control, policy, or action taken to counteract and attack, considered to be preventative (policies) and reactive. Examples include:

- Incident response.
- Antivirus updates or scans.

Sometimes a device or software can be a defense and a countermeasure, such as:

- Firewalls.
- Antivirus.
- Physical security.

Learning Activities

u01s1 - Studies

Readings

Use your *Network Defense and Countermeasures: Principles and Practices* text to read the following:

- Chapter 1, "Introduction to Network Security."
- Chapter 2, "Types of Attacks."

Skillsoft Resources

Use the Capella University Library to complete the following:

- Skillsoft. (n.d.). *CompTIA Cloud+ CV0-001: Cloud security* [Tutorial].
  - Under "Network Security Concepts," complete "Common Network Attacks."
- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
  - Complete "Network Hardening" and "Firewalls."
- Skillsoft. (n.d.). *Cybersecurity 101: Session & risk management: Asset, threats, and vulnerabilities* [Tutorial].
- Skillsoft. (n.d.). *SSCP domain: Risk, response, and recovery* [Tutorial].
  - Under "Risk and Incident Management," complete "Managing Risk and Identifying Vulnerabilities."

Use the Capella library to read the following:

- Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. Skillsoft Ireland.
  - Chapter 24, "Identifying and Defending Against Vulnerabilities."
- Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA Security+ and beyond* (fifth ed.) (Exam SY0-501). Skillsoft Ireland.
  - Chapter 1, "Introduction and Security Trends."

- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
  - Chapter 1, "Security and Risk Management."
  - Chapter 4, "Communication and Network Security."

Discussion Preparation

As noted in the syllabus, you will be working with a fictional hospital throughout the course to strengthen the security of its network infrastructure. In preparation for your first discussion in which you will discuss possible network attacks at the hospital, read the Anchor Hospital Scenario [DOCX].

u01s1 - Learning Components

- Identify types of network countermeasures.
- Identify common network attacks.
- Identify types of network defenses.
- Identify basic network vulnerabilities.

u01s2 - Software Preparation and Technology Access

In this course, you will be using software and technology to complete specific activities and assignments. Some software packages will be made available to you at no additional cost through Capella's subscription with Microsoft, and others 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 Windows Environment.

The software and technologies below are strongly recommended to support you in completing the course objectives. If you have access to other tools that you believe may still meet course requirements or if you have any difficulties accessing this resource or completing the related assignments, please contact your course faculty member to discuss potential alternatives.

If you use assistive technology or any alternative communication methods to access course content, please contact DisabilityServices@Capella.edu with any access-related questions or to request accommodations.

For this course, follow the instructions provided through the links below to download and install software or register for an account, as required.

Microsoft Software

- Visit Capella's Microsoft Software page for instructions on obtaining free Microsoft software.

- Identify the version of MS Visio that is compatible with your operating system.
- Download and install.

If you encounter any difficulties in the download and installation process, post a detailed question in Ask Your Instructor. Your instructor should be able to help you or point you in the right direction for the answers you need.

Additional Internet Resources

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

u01d1 - Common Network Attacks

For this discussion, review the Anchor Hospital Scenario (linked in Resources) and complete the following:

Discuss a common attack that might be perpetrated on the Anchor Hospital network infrastructure. How might this attack be conducted? What might be its goals? Identify a countermeasure to mitigate such an attack.

Response Guidelines

Read the posts of your peers and respond to at least two, offering comments that further the discussion or contribute to your peers' ideas.

Course Resources
Undergraduate Discussion Participation Scoring Guide
Anchor Hospital Scenario [DOCX]

u01d1 - Learning Components

- Identify types of network countermeasures.
- Identify common network attacks.

u01a1 - Identifying Network Security Components

Overview

Getting to know your network is an important first step in securing it. In this assignment you diagram the Anchor Hospital network, identifying its vulnerabilities and a significant threat that it might face.

Preparation

- Review the Anchor Hospital Scenario (linked in Resources).
- Identify an appropriate graphics or diagramming tool (such as Visio) to complete the assignment diagram.
- Refer to the Create a Network Diagram tutorial in Resources as needed.

Instructions

Complete the following:

- Create a diagram that accurately reflects the Anchor Hospital Network as defined in the scenario. There are several possible interpretations. The goal is to include all network components listed in the scenario and place them in reasonable locations. You will develop this diagram further in future assignments.
- Describe two network vulnerabilities and two countermeasures currently on the network.
- Identify and describe a significant threat to the Anchor Hospital network infrastructure given its current configuration. There is no single correct answer, but it is critical that you support your choice with strong rationale and evidence.

Additional Requirements

- Label your document clearly.
- Use an appropriate typeface and size, such as Times New Roman, 12 points, for body copy. Use double-spacing.
- Apply current APA style and formatting. An optional APA template is linked in Resources for your convenience.

Course Resources
Anchor Hospital Scenario [DOCX]
Create a Network Diagram
APA Paper Template
APA Style and Format

Unit 2 >> Firewalls

Introduction

In this unit you:

- Discuss firewall implementation.
- Configure a Windows Firewall in a lab.
- Select a proper position of a hardware-based firewall on the Anchor network and suggest possible reasons for the decision to use it as a replacement for Windows Firewall.

This unit introduces a major component of a secure network infrastructure: the firewall. Firewalls are the mainstay of network border security, as they provide protection from Internet and other intrusions. There are many software- and hardware-based firewall products available for various applications. Understanding how to leverage firewall technology without unduly affecting functionality and response time is important when configuring firewalls, as is their placement on the network. Firewalls are a critical network defense component, and understanding them is an essential for network security specialists.

Learning Activities

u02s1 - Studies

Readings

Use your *Network Defense and Countermeasures: Principles and Practices* text to read the following:

- Chapter 3, "Fundamentals of Firewalls."
- Chapter 4, "Firewall Practical Applications."

Use the Capella library and the Internet to read the following:

- Hu, H., Ahn, G.-J., & Kulkarni, K. (2010). FAME: A firewall anomaly management environment. In *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration* (pp. 17–26). New York, NY: ACM.
- Scarfone, K., & Hoffman, P. (2009). Guidelines on firewalls and firewall policy: Recommendations of the National Institute of Standards and Technology [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Skillsoft Resources

Use the Capella library to complete the following:

- Shannon, M. (2018). *CompTIA Security+ SY0-501: Components supporting organizational security* [Tutorial]. Skillsoft.
    - Complete the "Firewalls" tab.
- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
    - Complete the "Firewalls" tab, which covers types of firewalls and their network placement.
- Skillsoft. (n.d.). *Security fundamentals: Firewalls* [Tutorial].

Use the Capella library to complete the following:

- Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA Security+ and beyond* (fifth ed.) (Exam SY0-501). Skillsoft Ireland.
    - In Chapter 9, " Network Fundamentals," read "Security Device/Technology Placement."
    - In Chapter 10, "Infrastructure Security," read "Firewalls."
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
    - Review Chapter 4, "Communication and Network Security."

u02s1 - Learning Components

- Understand firewall hardware placement best practices.
- Explain how a hardware firewall protects a network.
- Understand differences between hardware and software firewalls.
- Explain how Windows firewall protects a network.

u02d1 - Firewall Change Control Process

Imagine you finally have your new firewall up and running. After much consultation with users, its governing rules are in place and functioning properly. However, you receive two requests for changes in the firewall during the first week:

1. The head of marketing would like the local newspaper to have daily network access to download employment ads from the marketing file server.
2. The firewall has broken the head of research and development's connection to a favorite website. He wants his access back and has asked for your help.

Discuss how you would respond to these requests. What kinds of procedures are needed to ensure that proper requests are implemented and inappropriate requests are denied?

Response Guidelines

Read the posts of your peers and respond to at least two, offering comments that further the discussion or contribute to your peers' ideas.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u02v1 - Lab: Configuring Windows Firewalls

Overview

In this lab you configure two Windows Firewall rules and test them to see if they were applied correctly. This lab takes approximately two hours.

Instructions

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

Select the linked title heading above to access a custom lab developed for this course.

1. Use the Assignment Template linked in Resources for your lab screenshots and assignment responses.
2. Follow the lab instructions carefully and complete Sections 1 and 2.
3. Take the following screenshots:
    - Section 1:
        - Part 2, Step 14.
        - Part 3, Step 3.
    - Section 2:
        - Part 2, Step 4.
        - Part 3, Step 2.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett Learning virtual labs, contact technical support via one of the following options:

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

Course Resources

Assignment Template [DOCX]

u02a1 - Selecting, Positioning, and Configuring a Firewall

Overview

As we have discussed, firewalls can be software or hardware based, and each has its pros and cons. In this assignment you identify an appropriate position for a hardware-based firewall on the Anchor Hospital network and explain why it was chosen to replace Windows Firewall.

Preparation

- Make sure you have completed the unit lab and saved your screenshots before beginning work on the assignment.
- Review the Anchor Hospital Scenario (linked in Resources) as needed.
- Refer to the Create a Network Diagram tutorial (linked in Resources) as needed.

Instructions

Populate the Lab Template (linked in Resources) with your screenshots and describe briefly but specifically what you learned from or observed in the lab.

Currently the Anchor Hospital network uses Windows Firewall. A decision has been made to switch to a hardware firewall solution. Complete the following:

- Position the new hardware for maximum effectiveness in the Anchor network to reflect the positioning. Explain your reasoning for its placement and update your network diagram from the Unit 1 assignment.
    - *Note:* Make sure you have responded to any instructor feedback on your diagram so you are working with an accurate and appropriate diagram.
- Suggest three plausible reasons why Anchor Hospital might switch to a hardware-based solution from Windows Firewall.
    - Explain how the change may enhance network security.

Additional Requirements

- Include your updated diagram and lab screenshots in the template as specified.
- Label your document clearly.
- Use an appropriate typeface and size, such as Times New Roman, 12 points, for body copy. Use double-spacing.
- Apply current APA style and formatting as appropriate.

Course Resources
Anchor Hospital Scenario [DOCX]
Create a Network Diagram
APA Style and Format
Assignment Template [DOCX]

Unit 3 >> Physical Security

Introduction

In this unit you:

- Discuss best practices for controls that enhance physical security.
- Use social engineering techniques to plan an attack in a lab.
- Identify weaknesses in Anchor Hospital physical security and suggest controls and a policy to mitigate them.

Unit 3 introduces principles of physical security and disaster recovery. Physical security includes many things, from door locks to personnel. Sometimes an organization's physical security may be its greatest IT vulnerability. Understanding how physical attacks occur, how to prevent them, and how to recover from them is an important part of infrastructure security.

Learning Activities

u03s1 - Studies

Readings

Use your *Network Defense and Countermeasures* text to read the following:

- Chapter 14, "Physical Security and Disaster Recovery."

Use the Internet to read the following:

- Covington, R. C. (2015, Jun 23). Physical security: The overlooked domain [Blog post]. Retrieved from https://www.csoonline.com/article/2939322/physical-security-the-overlooked-domain.html

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
  - Complete the "Physical Security" tab.

Use the Capella library to complete the following:

- Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA Security+ and beyond* (fifth ed.) (Exam SY0-501). Skillsoft Ireland.
  - Read Chapter 8, "Physical Security."
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
  - In Chapter 3, "Security Architecture and Engineering," read:
    - "Site and Facility Security."
    - "The Site Planning Process."
  - In Chapter 7, "Security Operations," read:
    - "Physical Security."
    - "Personal Safety Concerns."

u03s1 - Learning Components

- Understand principles of physical network security.
- Identify network security controls and the attacks they are designed to thwart.
- Identify policies that are effective to network defense.

u03d1 - Physical Security

Securing physical assets is an important and sometimes overlooked aspect of IT security.

Discuss, based upon your research or professional experience, best practices that are often employed to enhance physical security and prevent unauthorized access to network operations centers.

Response Guidelines

Read the posts of your peers and respond to at least two, offering comments that further the discussion or contribute to your peers' ideas.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u03d1 - Learning Components

- Identify network security controls and the attacks they are designed to thwart.

u03v1 - Lab: Using Social Engineering Techniques to Plan an Attack

Overview

In this lab you perform a social engineering attack. This lab will take approximately 2 hours.

Instructions

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

Select the linked title heading above to access a custom lab developed for this course.

1. Use the Assignment Template linked in Resources for your lab screenshots and your assignment responses.
2. Follow the lab instructions carefully and complete Sections 1 and 2.
3. Take the following screenshots:
    - Section 1: Hands-on Demonstration.
        - Part 1: Steps 7, 12, 15, 18, and 22.
    - Section 2: Applied Learning.
        - Part 1: Steps 2, 3, 8, and 11.
        - Part 2: Steps 3, 5, and 7.
        - Part 3: Steps 3, 12, 21, and 25.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett Learning virtual labs, contact technical support via one of the following options:

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

Course Resources

Assignment Template [DOCX]

u03a1 - Physical Security Recommendation

Overview

Physical security is often an overlooked area of IT security. Planning for and maintaining physical defense of IT assets is of paramount concern for IT security professionals.

In this assignment you identify weaknesses in Anchor Hospital's physical security and recommend a control to mitigate possible social engineering attacks.

Preparation

- Make sure you have completed the unit lab and saved your screenshots before beginning work on the assignment.
- Review the Anchor Hospital Scenario (linked in Resources) as needed.

Instructions

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template (linked in Resources). Be specific.

Anchor Hospital has vulnerabilities in its defense against social engineering attacks.

- Identify two significant attributes of the hospital's physical security that leave it vulnerable to a social engineering attack. Explain how each might be exploited. State any assumptions not explicitly defined in the scenario that are required to support your explanation.
- Suggest a nonpolicy control that effectively addresses the vulnerability and explain why it would be effective.
- Write a specific policy no longer than one page to address the vulnerability.

Additional Requirements

- Label your document clearly.
- Use an appropriate typeface and size, such as Times New Roman, 12 points, for body copy. Use double-spacing.
- Apply current APA style and formatting as appropriate.

Course Resources

Anchor Hospital Scenario [DOCX]
Assignment Template [DOCX]

Unit 4 >> Cloud Security

Introduction

In this unit you:

- Discuss essentials of cloud-hosted security.
- Complete an assignment in which you examine issues related to hosting medical data in the cloud.

Companies are increasingly using cloud services to host critical data and applications. Ensuring security in the cloud is vital and requires an understanding of which security must be used and what an organization must ask of a cloud hosting firm.

Note: There is no lab this week.

Learning Activities

u04s1 - Studies

Readings

Use the Internet to complete the following:

- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
  - Read pages 1–3.

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CompTIA Cloud+ CV0-002: Security technologies and automation techniques* [Tutorial].
- Skillsoft. (n.d.). *Moving business services into the cloud* [Tutorial].
  - Complete the tab "Adopting Cloud Services."

Use the Capella library to read the following:

- Anandamurugan, S., Priyaa, T., & Arvind Babu, M. C. (2017). *Cloud computing: An innovative technology for Linux and Android platforms*. Skillsoft Ireland.
  - Chapter 13, "Issues and Risks in Cloud Computing."
- Gupta, B. B., Agrawal, D. P., & Wang, H. (Eds.). (2019). *Computer and cyber security: Principles, algorithm, application, and perspectives*. Skillsoft Ireland.
  - Chapter 11, "Cryptography for Addressing Cloud Computing Security, Privacy, and Trust Issues."
- Vacca, J. R. (2017). *Security in the private cloud*. Skillsoft Ireland.
  - Chapter 1, "Private Cloud Computing Fundamentals."
  - Chapter 7, "Selecting the Appropriate Product."
  - Chapter 9, "Security in the Virtual Private Cloud."
- Willcocks, L., Venters, W., & Whitley, E. A. (2014). *Moving to the cloud corporation: How to face the challenges and harness the potential of cloud computing*. Skillsoft Ireland.
  - Chapter 4, "The Challenges."
  - Chapter 5, "Security and Privacy Concerns Revisited."

u04s1 - Learning Components

- Understand fundamentals of cloud hosted security.
- Identify cloud hosting compliance, regulatory and legal considerations.
- Identify important aspects and issues related to cloud hosted security.

u04d1 - Cloud Security

Imagine Anchor Hospital is researching cloud service providers such as AWS or Google to run some of its applications and store patient data. You are on the vetting team and are meeting with a representative from AWS to voice your security-related concerns. She asks you, "What are the two most important security concerns for you as the hospital's network security administrator?"

For this discussion, answer the question and pose two questions to the AWS rep, providing your rationale for asking them.

Response Guidelines

Read the posts of your peers and respond to at least two, offering comments that further the discussion or contribute to your peers' ideas.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u04d1 - Learning Components

- Understand fundamentals of cloud hosted security.

u04a1 - Cloud Vendor Security Considerations

Overview

Cloud hosting is becoming an increasingly attractive option for IT departments, but these providers must also confront security issues. In this assignment you consider cloud hosting security issues.

Scenario

Imagine you receive the following email from the Anchor Hospital CIO:

> Hi!
>
> I'm looking at options for hosting our applications and medical data in the cloud. Can you please give me your opinion on the pros and cons of cloud hosting for our needs? Data security is the priority but I'm also interested in other aspects of the migration. Could you please shoot me a memo to:
>
> - Explain the data security-related pros and cons of a move to the cloud.
> - Identify compliance, regulatory, or legal watch-outs for the move and tell me which is the greatest concern.
> - List critical security-related criteria for choosing a cloud host. Which one do you think is most important for safeguarding patient data?
> - Pick a commercial hosting service (AWS, Azure, Google, other?) and explain how it meets one of your criteria.
>
> Thanks,
>
> Mindy

Instructions

Write a memo to the CIO detailing the pros and cons of hosting Anchor Hospital medical data in the cloud as specified in the scenario above. Make sure to:

1. Explain the security-related pros and cons of hosting medical data in the cloud.
2. Explain threerelevant cloud hosting compliance, regulatory, or legal considerations.
3. Identify fivesecurity-related criteria most critical when selecting an appropriate cloud host provider. Detail one of them.
4. Explain how your chosen cloud hosting solution meets one of your criteria.

Make sure to support your work with professional resources.

Additional Requirements

- Clearly label your memo in a Word document. An optional Microsoft memo template is linked in Resources for your convenience.
- Double-space lines.
- Use current APA style and formatting for any outside sources used to support your assertions.

Course Resources
Memos
APA Style and Format

Unit 5 >> Intrusion Detection and Signature Analysis

Introduction

In this unit you:

- Discuss IDS-related topics.
- Analyze protocols with Wireshark in a lab.
- Submit an assignment in which you respond to an IDS alert and suggest controls to address it and other types of attacks.

Intrusion detection systems (IDS) are the mainstay of network traffic analysis for anomalies. With the emergence of spyware, there has been renewed interest in IDS. An IDS screens items coming into various vectors including legitimate ports such as port 80. An IDS is best managed through a central console, which allows an administrator to maintain the broad perspective that confers an advantage over the "one device at a time"

approach. But intrusion detection is not without challenges and can be resource-intensive until it has been fine-tuned. Understanding the basics of intrusion detection is key to effective network infrastructure traffic monitoring.

Learning Activities

u05s1 - Studies

Readings

Use your *Network Defense and Countermeasures: Principles and Practices* text to read the following:

- Chapter 5, "Intrusion-Detection Systems."

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
  - Complete the "Common Threats and Vulnerabilities" tab.

Use the Capella library to read the following:

- Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. Skillsoft Ireland.
  - Chapter 4, "Understanding Intrusion-Detection and Reporting Systems."
- Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA Security+ and beyond* (fifth ed.) (Exam SY0-501). Skillsoft Ireland.
  - Chapter 13, "Intrusion Detection Systems and Network Security."
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
  - Chapter 5, "Identity Access Management."
- Pathan, A. K. (Ed.). (2014). *The state of the art in intrusion prevention and detection*. Skillsoft Ireland.
  - Chapter 2, "Network Traffic Monitoring and Analysis."

u05s1 - Learning Components

- Recognize the significance and sources of IDS alerts.
- Understand fundamental IDS functions and methods.
- Understand denial of service attack fundamentals.
- Understand how intrusion detection systems function on internal networks.
- Identify controls that mitigate denial of service attacks.

u05d1 - IDS Best Practices

Intrusion detection systems are increasingly important for detecting network attacks. While the choice of a tool and its configuration are critical, so too is how the system is managed and operated.

Discuss one of the following based on research or your own experience:

- Best practices for conducting ongoing intrusion detection on a corporate network.
- IDS types and their intended applications.
- How an IDS helped thwart an attack. How did it work with other systems?

Response Guidelines

Read the posts of your peers and respond to at least two, offering comments that further the discussion or contribute to your peers' ideas.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u05d1 - Learning Components

- Understand fundamental IDS functions and methods.

u05v1 - Lab: Analyzing Protocols With Wireshark

Overview

In this lab you analyze network traffic using Wireshark by capturing network traffic and viewing files at the packet level. This lab takes approximately 2 hours.

Instructions

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

Select the linked title heading above to access a custom lab developed for this course.

1. Use the Assignment Template linked in Resources to enter your lab screenshots and assignment responses.
2. Following the lab instructions carefully, complete Sections 1 and 2.
3. Take the following screenshots:
    - Section 1: Hands-On Demo

        - Part 1: Step 15.
        - Part 2: Steps 7 and 19.
    - Section 2: Applied Learning
        - Part 1: Steps 13 and 16.
        - Part 2: Steps 16, 21, 24, 27, and 40.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett Learning virtual labs, contact technical support via one of the following options:

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

Course Resources

Assignment Template [DOCX]

u05a1 - Intrusion Detection and Control

Overview

An IDS looks at packets entering and exiting the network. If the IDS detects packet anomalies, it alerts network security staff so countermeasures can be initiated.

In this assignment, you respond to an IDS alert and suggest controls to address it and other types of attacks.

Instructions

If you have not done so, complete the unit lab and save your screenshots in the Assignment Template (linked in Resources). Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template. Be specific.

Complete the following:

Part 1

Imagine the Anchor Hospital IDS is sending the following alert to the administration console with unexpected frequency (every two minutes):

2019-02-15 14:33:18.528 [1:19559:5] INDICATOR-SCAN Denial of service attempt [Classification: activity] [Priority: 1] {TCP} 200.200.200.11:64757 -> 192.168.128.157:22

Due to the abnormally high volume (and the fact that the IDS was recently reconfigured), you suspect that your IDS may be returning false alerts.

- Describe investigative actions that would confirm or deny your suspicion.

Part 2

Imagine that you determine that the high number of alerts was not false but a denial of service (DoS) attack.

- Identify two controls to mitigate the attack and explain why each is appropriate.

Part 3

You now recognize the importance of network monitoring and are concerned about the possibility of internal attacks as well.

- Explain where you chose to place the IDS agent or agents on the network to maximize effectiveness against internal attacks.
- Update your network diagram to reflect the position of each IDS agent and add it to the template.

Additional Requirements

- Label your document clearly.
- Use an appropriate typeface and size, such as Times New Roman, 12 points, for body copy. Use double-spacing.
- Apply current APA style and formatting as appropriate.

Course Resources
Assignment Template [DOCX]
APA Style and Format

Unit 6 >> VPN Security

Introduction

In this unit you:

- Discuss what to do when a VPN is compromised.
- Explore social engineering and reverse social engineering attacks, implement countermeasures, and perform an attack using social engineering in a lab.
- Compare VPN protocols and decide which one is most appropriate for Anchor Hospital.

This unit provides an in-depth exploration of virtual private networks (VPN) technology. VPNs offer some of the most secure methods of communicating privately over a public network. VPN technology offers a wide variety of options, including the use of encryption to create a private tunnel through a public network. Proper support of this technology includes understanding the points of vulnerability and the available controls to mitigate risk. Network security professionals benefit from understanding the range of VPN options and how to implement them properly.

Learning Activities

u06s1 - Studies

Readings

Use your *Network Defense and Countermeasures* text to read the following:

- Chapter 7, "Virtual Private Networks."

Use the Internet to read the following:

- Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2008). Guide to SSL VPNs: Recommendations of the National Institutes of Standards and Technology [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf

Skillsoft Resources

Use the Capella library to complete the following:

- Clarke, G. E. (2018). *CompTIA network+ certification study guide* (7th ed.). Skillsoft Ireland.
  - Chapter 11, "Remote Access and VPN Connectivity."
- Gibson, D. (2018). *SSCP Systems security certified practitioner all-in-one exam guide* (third ed.). Skillsoft Ireland.
  - Chapter 4, "Advanced Networking and Communications."
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
  - Review Chapter 4, "Communications and Network Security."

Use the Capella library to complete the following:

- Shannon, M. (2018). *CompTIA Security+ SY0-501: Components supporting organizational security* [Tutorial]. Skillsoft.

- Complete the following tabs:
  - VPN Concentrators.
  - NIDS and NIPS.

u06s1 - Learning Components

- Identify security issues relevant to VPN protocols.
- Explain fundamental qualities of Layer 2 Tunneling, SSL Tunneling, and Open VPN protocols.
- Identify considerations important to VPN adoption.
- Understand how a VPN integrates with other parts of a company network.
- Understand the basic features and requirements of VPN protocols.

u06d1 - VPN Security

Imagine you are examining firewall logs and look up to see the chief information officer (CIO) walking past your office. Then you notice that the CIO's VPN account is logged in to the network and the associated user is engaged in highly questionable behavior. You suspect that the CIO's teenage son, Terrible Timmy, has compromised your CIO's laptop.

Discuss what action you will take to address the compromise and ensure that the hole has been closed.

Response Guidelines

Read the posts of your peers and respond to at least one. Respond to a learner who has not yet received feedback, providing a careful review of his or her work.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u06d1 - Learning Components

- Identify security issues relevant to VPN protocols.

u06v1 - Lab: Attacking a Virtual Private Network

Overview

In this lab you explore social engineering and reverse social engineering attacks, implement countermeasures, and perform an attack using social engineering. This lab takes approximately two hours.

Instructions

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

Select the linked title heading above to access a custom lab developed for this course.

1. Save your lab screenshots and assignment responses in the Assignment Template (linked in Resources).
2. Follow the lab instructions carefully and complete Sections 1 and 2.
3. Take the following screenshots:
    - Section 1: Hands-On Demonstration
        - Part 1: Steps 10 and 16.
        - Part 2: Step 4.
    - Section 2: Applied Learning
        - Part 1: Steps 24 and 38.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett Learning virtual labs, contact technical support via one of the following options:

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

Course Resources
Assignment Template [DOCX]

u06a1 - VPN Security Solution

Overview

VPN solutions are based on protocols such as Layer 2 tunneling (L2TP), secure socket layer (SSL) tunneling, and OpenVPN. In this assignment you compare the protocols and choose one for Anchor Hospital.

Scenario

Anchor Hospital wants to add a VPN to serve the remote connections for off-site employees. It is your job to evaluate the strengths and weaknesses of VPN protocols and determine which is most appropriate for Anchor Hospital. Your options are:

- Layer 2 tunneling (L2TP).
- Secure socket layer-based tunneling (SSL).
- OpenVPN.

Instructions

If you have not done so, complete the unit lab and populate the Assignment Template containing your screenshots. Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template. Be specific.

Complete the following:

- Compare the three VPN protocols to highlight their appropriate application, features, pros and cons, and other distinctions.
- Identify appropriate criteria for VPN selection for Anchor Hospital.
- Choose the most appropriate solution and provide a rationale for your decision.

Course Resources
Assignment Template [DOCX]

Unit 7 >> Incident Response and Countermeasures

Introduction

In this unit you:

- Discuss security countermeasures.
- Identify, contain, and eradicate the attack and write the incident response report in a lab.
- Respond to a network attack and complete an incident response report detailing the incursion and your actions.

This unit introduces techniques used by hackers and how to respond to them. You examine strategies and apply countermeasures against common attacks and explore how hacking tools work. You also explore viruses, Trojan horses, adware, and spyware.

Incident Response

Will your company know how to respond if an attack occurs? Every company should have a plan to deal with a variety of security incidents. Included in the plan are procedures for containment and countermeasures. Reporting an incident accurately and completely is also an important part of incident response, as it can inform future security responses and planning.

Learning Activities

u07s1 - Studies

Readings

Use your *Network Defense and Countermeasures* text to read the following:

- Chapter 9, "Defending Against Virus Attacks."
- Chapter 10, "Defending Against Trojan Horses, Spyware and Adware."
- Chapter 15, “Techniques Used by Attackers."

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
  - Complete the "Incident Management" tab.
- Skillsoft. (n.d.). *Cybersecurity 101: Session & risk management: Asset, threats, and vulnerabilities* [Tutorial].
- Skillsoft. (n.d.). *SSCP domain: Risk, response, and recovery* [Tutorial].
  - Under "Risk and Incident Management," "Managing Risk and Identifying Vulnerabilities," complete the following:
    - "Detecting and Analyzing Security Incidents."
    - "Containing and Eradicating Security Incidents."
    - "Managing and Handling Security Risks and Incidents."

Use the Capella library to complete the following:

- Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA Security+ and beyond* (fifth ed.) (Exam SY0-501). Skillsoft Ireland.
  - Chapter 15, "Types of Attacks and Malicious Software."
  - Chapter 22, "Incident Response."
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
  - Review the following:
    - Chapter 5, "Identity and Access Management."

- Chapter 7, "Security Operations."

u07d1 - Countermeasures

Countermeasures generally include activities that can prevent incidents from recurring. Some in the security community would include counterattack among the countermeasures available to an incident response team.

Discuss the following:

- Activities that constitute countermeasures.
- Potential advantages of engaging in countermeasures.
- Potential challenges to engaging in countermeasures.
- Legal implications of engaging and aggressive counterattack as a countermeasure.

Response Guidelines

Read the posts of your peers and respond to at least two, offering comments that further the discussion or contribute to your peers' ideas.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u07v1 - Lab: Investigating and Responding to Network Security Incidents

Overview

In this lab you identify, contain, and eradicate an attack and write the incident response report. This lab will take approximately two hours.

Instructions

Read the requirements for all related course activities before completing this lab, taking notes to help you complete those activities.

Select the linked title heading above to access a custom lab developed for this course.

1. Use the Lab Template linked in Resources for this assignment.
2. Follow the lab instructions carefully, completing Sections 1 and 2.
3. Take the following screenshots from:
    - Section 1: Hands-On Demonstration
        - Part 2: Step 7.
        - Part 3: Steps 2 and 10.
    - Section 2: Applied Learning
        - Part 2: Step 8.
        - Part 3: Steps 2 and 9.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett Learning virtual labs, contact technical support via one of the following options:

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

Course Resources
Lab Template [DOCX]

u07a1 - Incident Response and Report

Overview

In this assignment you write an incident response report—a critical skill in IT security.

Scenario

Imagine that you are on duty as a first responder in the Anchor Hospital IT department. You receive complaints that users cannot send or receive email. Your initial investigation reveals that your network has been compromised by a denial of service attack (DoS). It is your job to identify systems that could be impacted, contain the attack, deploy immediate countermeasures, complete an incident response report (note you fill out the report as if you had actually taken the steps you are advocating), and recommend measures to prevent recurrence.

Instructions

- Populate the Lab Template (linked in Resources) with your screenshots and describe briefly but specifically what you learned from or observed in the lab.
- Use the Incident Response Report Template (linked in Resources) to document your actions in the wake of the incident described above. By completing it you address the following assignment criteria:
  - Identify systems that are likely to be affected by a DoS attack.
  - Describe appropriate steps to contain the DoS attack.
  - Identify two countermeasures and detail why they are appropriate.
  - Describe a noncountermeasure control that is effective for mitigating similar future attacks.
- Submit the completed Lab and Incident Response Report Templates.

Course Resources
Incident Response Form Template [DOCX]
Lab Template [DOCX]

Unit 8 >> Policy, Regulatory, and Legal Considerations

Introduction

In this unit you:

- Discuss security-related ethical issues.
- Back up and restore data, ensure access controls, configure a host-based firewall, and scan for vulnerabilities in a lab.
- Update the Anchor Hospital password policy and consider associated risks and ethics in the unit assignment.

This unit introduces some of the major regulations and policies related to network security. The intent of these regulations is to govern data protection. The type of organization often determines which policies and regulations must be followed. Understanding these policies and regulations is necessary to determining the controls an organization needs and how to regulate them.

Learning Activities

u08s1 - Studies

Readings

Use your *Network Defense and Countermeasures* text to read the following:

- Chapter 11, "Security Policies."

Use the Internet to complete the following:

- Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D. I. (2008). An introductory resource guide for implementing the Health Insurance Portability Act (HIPAA) security rule [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
  - Read pages 6–9, 15–27, 35–39, 47–48, 52–53.

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
  - Under the tab "Security Concepts," complete the section labeled "Security Policy."
- Skillsoft. (n.d.). *SSCP domain: Security operations and administration part 1* [Tutorial].
  - Under the tab "Security and Business Practices," complete "Security Objectives and Ethics."
  - Under the tab "Confidentiality, Information and Systems Security," complete the following sections:
    - Security Policy Documents and Life Cycle.
    - Standards and Guidelines.

Use the Capella library to complete the following:

- Conklin, W. A., White, G., Cothren, C., Davis, R., & Williams, D. (2018). *Principles of computer security: CompTIA Security+ and beyond* (fifth ed.) (Exam SY0-501). Skillsoft Ireland.
  - Chapter 24,"Legal Issues and Ethics."
  - Chapter 25, "Privacy."
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
  - In Chapter 1, "Security and Risk Management," review the following sections:
    - "The Crux of Computer Crime Laws."
    - "Privacy."
    - "Data Breaches."
    - "Ethics."

u08s1 - Learning Components

- Understand password policy best practices.
- Examine ethical issues of privacy and hacking.
- Explain basic legal issues regarding access of patient data.

- Explain how password policy impacts network and data security.

u08d1 - Ethical Hacking

Sometimes it is necessary to conduct so-called white hat operations, which entail hacking by "the good guys." This sounds simple enough but there are ethical implications for such actions.

Discuss the following:

- What is "ethical hacking?" What is an example of it?
- Should security personnel have unfettered access to data or systems they are entrusted to protect?
- What is an IT security-related situation in which you faced (or researched) an ethical dilemma?
  - How did you approach it?
  - How was it resolved?

Response Guidelines

Read the posts of your peers and respond to at least two with comments or arguments that further the discussion or contribute to your peers' ideas.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u08d1 - Learning Components

- Examine ethical issues of privacy and hacking.

u08v1 - Lab: Applying Regulatory Compliance Standards

Overview

In this lab you implement policies related to several regulations. You back up and restore data, ensure access controls, configure a host-based firewall, and scan for vulnerabilities. This lab will take approximately 2 hours.

Instructions

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

Select the linked title heading above to access a custom lab developed for this course.

1. Follow the lab instructions carefully and complete Sections 1 and 2 of the Lab Template (linked in Resources).
2. Take the following screenshots:
    - Section 1: Hands-on Demonstration:
        - Part 1: Step 32.
        - Part 2: Steps 15, 22, 33, and 46.
        - Part 4: Step 35.
        - Part 5: Steps 5 and 12.
    - Section 2: Applied Learning:
        - Part 1: Steps 11 and 16.
        - Part 2: Steps 19 and 33.
        - Part 3: Step 12.
        - Part 4: Step 17.
        - Part 5: Step 5.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett virtual labs, contact technical support via one of the following options:

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

Course Resources
Lab Template [DOCX]

u08a1 - Password Security Policy

Overview

As technology evolves, policies designed to regulate technologies also age and become obsolete. In this assignment, you update the Anchor Hospital password policy and consider associated risks and ethics.

Scenario

Anchor Hospital has just performed a security risk analysis. One finding of the risk analysis is that the company's password policy is outdated. You are tasked with updating the policy to align with current best practices and standards.

During the risk assessment, one of your colleagues tested the current password protections using a brute-force method for breaking passwords. Some might consider this ethical hacking. But your associate went so far as to exploit a password to prove the inadequacy of the existing password requirements. During this attack, he gained access to restricted and confidential patient data.

Instructions

Begin by reviewing Current Password Policy (linked in Resources).

Populate the Lab Template with your screenshots to complete the lab documentation, briefly describing what you learned from or observed in the lab. Be specific.

Update and rename the "Current Password Policy" document. Create a separate Word document for bullets 2 and 3.

Complete the following with respect to the scenario above:

1. Update **four** significant elements of the password security policy to reflect current password security best practices.
    - Save the document as "Proposed Password Security Policy."
    - Substantiate your proposed changes with references to appropriate sources.
    - Use the "track changes" feature in Word or strike out language to be replaced and add updated language in bold red type.
2. Analyze two possible legal ramifications of the unauthorized hacking of patient data.
3. Analyze if the unauthorized hacking constitutes an ethical breach. Make sure to substantiate your opinions with proper references.
4. Explain how this risk analysis (as presented) impacts current or future information security at the company.

Additional Requirements

1. Submit the Lab Template with your screenshots and narrative.
2. Submit your completed Updated Password Policy.
    - Reference a minimum of two professional sources.
3. Submit a two-page, double-spaced Word document for bullets 2–4. It should include:
    - Current APA formatting and style.
    - References from three or more professional sources.

Course Resources

Current Password Policy [DOCX]

Lab Template [DOCX]

Unit 9 >> Defending With Encryption

Introduction

In this unit you:

- Discuss your experience with encryption.
- Apply encryption and hashing techniques to secure communications in a lab.
- Compare encryption methods and recommend one for Anchor Hospital in an assignment.

This unit introduces the fundamentals of data encryption, including methods and best practices for protecting data in its various states and locations. Communications, moving data, and data at rest are important areas that must be encrypted. This unit involves learning techniques to use in securing data and communications.

Learning Activities

u09s1 - Studies

Readings

Read the following in your *Network Defense and Countermeasures* text:

- Chapter 6, "Encryption Fundamentals."

Use the Internet to complete the following:

- Rose, S., Nightingale, J. S., Garfinkel, S. L., & Chandramouli, R. (2019). NIST special publication 800-177 revision 1: Trustworthy email [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf
  - Pages 15–24.
  - Pages 80–83.

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CompTIA Cloud+ CV0-001: Cloud security* [Tutorial].

- Lesson 3, "Encryption."

- Skillsoft. (n.d.). *Cybersecurity 101: Auditing and incident response* [Tutorial].
  - "Securing Applications."
  - "Implement File Hashing."

Use the Capella library to complete the following:

- Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. Skillsoft Ireland.
  - Chapter 22, "Protecting Data Moving Through the Internet."
- Harris, S., & Maymi, F. (2019). *CISSP all-in-one exam guide* (eighth ed.). Skillsoft Ireland.
  - Chapter 3, "Security Architecture and Engineering."

u09s1 - Learning Components

- Identify applications, features, and other foundational aspects of Asymmetric Encryption.
- Identify issues involved with encryption implementation.
- Identify applications, features, and other foundational aspects of PKI.
- Explain applications, features, and other foundational aspects of Asymmetric Encryption and PKI.

u09d1 - Encryption

Choose *one* of the following to discuss based on your experience or research:

1. Describe an instance in which encryption was used.
   - What type was it?
   - What considerations drove its adoption?
   - Was it effective?
   - How much effort was required to deploy and maintain it?
2. Discuss your opinion on whether individuals or businesses should be able to encode their communications with sophisticated encryption methods that can stymie law enforcement or other investigative procedures.

Response Guidelines

Read the posts of your peers and respond to at least two with comments or arguments that further the discussion or contribute to your peers' ideas.

Course Resources

Undergraduate Discussion Participation Scoring Guide

- Identify issues involved with encryption implementation.

u09v1 - Lab: Applying Encryption and Hashing Techniques for Secure Communications

Overview

In this lab you apply common encryption techniques to ensure confidentiality, integrity, and authentication. You send a secure message and compare hash tags of an original file and a generated file. This lab takes approximately two hours.

Instructions

Read the requirements for all related course activities before completing this lab and take notes to help you complete those activities.

Select the linked title heading above to access a custom lab developed for this course.

1. Use the Assignment Template linked in Resources for your lab screenshots and assignment responses.
2. Follow the lab instructions carefully and complete Sections 1 and 2.
3. Take the following screenshots:
    - Section 1: Hands-on Demo
        - Part 2: Steps 4, 7, 11, 14, and 15.
        - Part 4: Steps 13 and 21.
        - Part 5: Step 6.
        - Part 6: Step 19.
    - Section 2: Applied Learning
        - Part 2: Steps 6 and 14.
        - Part 3: Step 7.
        - Part 4: Step 17.
        - Part 5: Step 12.
        - Part 6: Step 19.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett virtual labs, contact technical support via one of the following options:

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

Assignment Template [DOCX]
Lab: Applying Encryption and Hashing Techniques for Secure Communications

u09a1 - Defending With Encryption

Overview

Data exists in three states: at rest, in motion (or *transit*), and in use, each of which must be protected. Encryption is one of the tools commonly used to protect data in each state.

In this assignment you respond to a risk assessment finding that sensitive data at rest on a medical patient server are unencrypted.

Scenario

Anchor Hospital's electronic record management (ERM) system's sensitive data on one of the servers was found to be vulnerable by the conductors of the risk assessment, who recommended encrypting sensitive patient data. This is not small task and you recognize that you must conduct research to define an encryption practice for protecting company data for others' implementation.

Instructions

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template. Be specific.

Based on the above scenario, address the following:

1. Compare asymmetric encryption to public key infrastructure (PKI), considering applications, requirements, implementation considerations, and so on.
2. Recommend the most appropriate encryption method for securing Anchor's sensitive at-rest data. Justify your decision with specific rationale and supporting resources.
3. Describe three considerations (hardware, software, processes, policies, other) that should guide planning and implementing your solution.

Introduction

In this unit you:

- Discuss network attacks.
- Complete a lab in which you explore risks, threats, and vulnerabilities with cloud computing, social networking, and mobile computing.
- Assess a company's network infrastructure exposures in an assignment.

The success of a security project stems from your ability to evaluate the risks to the organization's information assets. It is impossible to develop a secure infrastructure without identifying what is to be protected and what it is being protected against.

Understanding the basics of conducting an enterprise risk assessment is one of the fundamentals of sound security practices. A comprehensive risk assessment evaluates the degree of risk, which is generally assessed as the potential for a specific risk to occur, combined with the impact on the organization should it occur. The items associated with the highest risk and the highest impact to the organization are areas of particular concern that must be addressed.

Learning Activities

u10s1 - Studies

Readings

Use your *Network Defense and Countermeasures* text to read the following:

- Chapter 12, "Assessing System Security."

Use the Internet to complete the following:

- National Institute of Standards and Technology (NIST). (2012). NIST special publication 800-30 r1: Guide for conducting risk assessments [PDF]. Available from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
  - Read pages 4–17.
- National Institutes of Standards and Technology (NIST). (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy [PDF]. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
  - Read pages 6–20.

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CompTIA Network+ N10-006: Network security* [Tutorial].
  - In Lesson 1, "Security Concepts," complete "Vulnerability Scanning and Penetration Testing."
- Skillsoft. (n.d.). *Cybersecurity 101: Session & risk management: Asset, threats, and vulnerabilities* [Tutorial]."
  - Complete "Risk Management" and "Map Risks to Risk Treatments" as well.
- Skillsoft. (n.d.). *SSCP domain: Risk, response, and recovery* [Tutorial].
  - In Lesson 1, "Risk and Incident Management," complete the following:
    - "Improving Risk Management Systems."
    - "Mitigating Risks."

u10s1 - Learning Components

- Identify the common types of risks faced by network infrastructures.
- Identify causes and levels of potential network exposure.
- Understand the degree to which network exposures can impact a network.
- Identify network controls appropriate for common network exposures.

u10d1 - Risks and Exposures

Choose one of the following to address in this discussion:

1. A major security threat currently facing a typical corporate network infrastructure.
   - Explain why you think it is so serious.
   - Identify parts of a typical network that are vulnerable to it.
2. An example of a network attack from the news or your own experience.
   - Identify the problems it caused and how it was mitigated or remedied.

Response Guidelines

Read the posts of your peers and respond to at least two with comments or arguments that further the discussion or contribute to your peers' ideas.

Course Resources
Undergraduate Discussion Participation Scoring Guide

- Identify the common types of risks faced by network infrastructures.

u10v1 - Lab: Recognizing Risks and Threats Associated With Emerging Technologies

Overview

This lab requires you to explore risks, threats, and vulnerabilities with cloud computing, social networking, and mobile computing.

Instructions

Read the requirements for all related course activities before completing this lab. Take notes as needed to help you complete those activities. The lab should take approximately 2 hours.

Select the linked title heading above to access a custom lab developed for this course.

- Follow the lab instructions carefully and complete Sections 1 and 2 of the Lab Template (linked in Resources).
- Take the following screenshots from Section 2:
  - Part 2: Steps 26 and 51.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing Jones and Bartlett virtual labs, contact technical support using one of the following options:

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

Course Resources
Lab Template [DOCX]

u10a1 - Risk Assessment and Mitigation

Overview

Evaluating a company's network security infrastructure is a complex undertaking that should include risk and vulnerability assessment (including ranking their severity), as well as mitigation actions, procedural controls, and supporting policies.

In this assignment you assess the risk faced by Anchor Hospital network infrastructure as detailed in the course project scenario.

Instructions

Populate the Lab Template with your screenshots to complete the lab documentation. Make sure you have included the specified screenshots in your document. Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots. Be specific.

Use the Risk Assessment Template (linked in Resources) to complete a risk assessment of Anchor Hospital's network infrastructure. Its appearance and content should be professional and refined. Your assessment should do the following:

- Describe four significant exposures (risks and or vulnerabilities) faced by the company's network infrastructure.
- Assess the likelihood and potential impact severity of each exposure.
- Describe what you believe would be the most effective control for addressing one of the four identified exposures through each of the following ways:
    - Mitigation.
    - Procedural.
    - Policy.

Submit your completed Lab Template and Risk Assessment Template.

Course Resources
Anchor Hospital Scenario [DOCX]
Risk Assessment Template [DOCX]