Preview: IAS5010 : IT Security Fundamentals

Syllabus

Course Overview

This course introduces the fundamentals of Information Assurance Security by examining security risks, technologies, concepts, principles, and issues. It provides opportunities to assess and mitigate specific points of network vulnerability using information security tools, policies, and the foundational concepts of cyber-defense and information assurance.

Learners apply network security concepts and frameworks in labs that provide hands-on experience with security tools, devices, and practices to identify and address network risks. A network scenario provides the opportunity to apply skills and knowledge to identifying and mitigating common vulnerabilities in a specified network.

Technology Resources

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

Kaltura Activities

As part of this course, you are required to record video presentations using Kaltura or similar software. Refer to Using Kaltura [PDF] for more information about this courseroom tool.

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

Course Competencies **(Read Only)**

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

1. Analyze networks and their security risks.

2. Explain network security technologies, concepts, and issues.
3. Apply network security concepts and frameworks.
4. Install, configure, and run network security management tools.
5. Communicate effectively.

Course Prerequisites

There are no prerequisites for this course.

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.

Hardware

Capella University requires learners to meet certain minimum computer requirements. The following hardware may go beyond those minimums and is required to complete learning activities in this course. **Note:** If you already have the following hardware, you do not need to purchase it. Visit the Course Materials page on Campus for more information.

Kaltura Hardware

Headset with microphone

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.

- Araújo, J. D., Rodrigues, D. d. A., de Melo, L. S., & Abdelouahab, Z. (2015). EICIDS-elastic and internal cloud-based detection system. *International Journal of Communication Networks and Information Security, 7*(1), 34–49.
- Armour, M. (2015). Talking about a (business continuity) revolution: Why best practices are wrong and possible solutions for getting them right. *Journal Of Business Continuity & Emergency Planning, 9*(2), 103–111.
- Ayub, K., & Zagurskis, V. (2015). Technology implications of UWB on wireless sensor network-A detailed survey. *International Journal of Communication Networks and Information Security, 7*(3), 147–161.
- Baham, C., Hirschheim, R., Calderon, A. A., & Kisekka, V. (2017). An agile methodology for the disaster recovery of information systems under catastrophic scenarios. *Journal Of Management Information System, 34*(3), 633–663.

- Bahtiyar, Ş. (2016). Anatomy of targeted attacks with smart malware. *Security & Communication Networks, 9*(18), 6215–6226.
- Barthe, G., Grégoire, B., Heraud, S., Olmedo, F., & Zanella-Béguelin, S. (2016). Verified indifferentiable hashing into elliptic curves. *Journal Of Computer Security, 21*(6), 881–917.
- Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P., & Mauro Madeira, E. R. (2015). Virtual network security: Threats, countermeasures, and challenges. *Journal of Internet Services and Applications, 6*(1), 1–19.
- Bhutta, M. N., Cruickshank, H., & Sun, Z. (2016). An efficient, scalable key transport scheme (ESKTS) for Delay/Disruption tolerant networks. *Wireless Networks, 20*(6), 1597–1609.
- Bou-Harb, E., Debbabi, M., & Assi, C. (2014). On fingerprinting probing activities. *Computers & Security, 43*, 35–48.
- Das, A. (2015). A secure and efficient user anonymity-Preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. *Wireless Personal Communications, 82*(3), 1377–1404.
- Denton, P. D., & Maatgi, M. K. (2016). The development of a work environment framework for ISO 9000 standard success. *The International Journal of Quality & Reliability Management, 33*(2), 231–245.
- El uahhabi, Z., & El bakkali, H. (2016). Calculating and evaluating trustworthiness of certification authority. *International Journal of Communication Networks and Information Security, 8*(3), 136–146.
- Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal Of Business Continuity & Emergency Planning, 11*(2), 163–173.
- Hartley, R. D. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management, 24*(4), 95–104.
- Jaheel, H. L., Zou, B., & Jaheel, A. L. (2015). Design and implementation steganography system by using visible image. *International Journal On Smart Sensing & Intelligent Systems, 8*(2), 1011–1030.
- Jingguo, W., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly, 39*(1), 91–A7.
- Joshi, C., & Singh, U. K. (2017). Information security risks management framework–A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128–137.
- Kalsi, T. (2017). Nmap: Network security scans. *Linux Format*, (219), 76–77.
- Madhavapeddy, A., & Scott, D. J. (2014). Unikernels: The rise of the virtual library operating system. *Communications Of The ACM, 57*(1), 61–69.
- Marion, T. J., Reid, M., Hultink, E. J., & Barczak, G. (2016). The influence of collaborative IT tools on NPD. *Research Technology Management, 59*(2), 47–53.
- Masmoudi, K., & Afifi, H. (2008). Building identity-based security associations for provider-provisioned virtual private networks. *Telecommunication Systems, 39*(3-4), 215–222.
- Parkyn, J. (2018). Wireless network scanning tools. *Web User*, (443), 48–49.
- Phan, R. C. -W. (2011). Non-repudiable authentication and billing architecture for wireless mesh networks. *Wireless Networks, 17*(4), 1055–1061.
- Rooney, J. J. (2017). A holistic approach to identify, understand, and mitigate risk. *The Journal for Quality and Participation, 40*(1), 39–40.
- Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165–176.

- Shannon, M. (n.d.). CompTIA CASP CAS-003: Organizational Security and Privacy Policies [Video]. Skillsoft Ireland.
- Singh, G., Goyal, S., & Agarwal, R. (2015). Intrusion detection using network monitoring tools. *IUP Journal of Computer Sciences, 9*(4), 46–58.
- Singh, G., Kaur, R., & Kaur, A. (2016). An approach to detect vulnerabilities in web-based applications. *International Journal of Advanced Research in Computer Science, 7*(1).
- Tao, L., Ning, X., Chunqiu, Z., Wubai, Z., Li, Z., Yexi, J., & Iyengar, S. S. (2017). Data-driven techniques in disaster information management. *ACM Computing Surveys*, *50*(1), 1–45.
- Tsoukalos, M. (2016). Wireshark: Analyse traffic. *Linux Format*, (218), 80–83.
- Wu, Z., Cai, M., Liang, S., & Zhang, J. (2014). An approach for prevention of MitM attack based on rogue AP in wireless network. *Sensors & Transducers, 183*(12), 162–171.

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.

- Alexander, A. (2015). Wireshark Tutorial for beginners [Video]. Retrieved from https://www.youtube.com/watch?v=TkCSr30UojM
- Hnatiw, A. (2017). A guide to implementing the top ten security principles for business. Retrieved from https://blog.securitycompass.com/are-you-following-the-top-ten-security-principles-for-business-9c28cf9ccd50/
- Martin, J. (2017). 7 things your IT disaster recovery plan should cover. Retrieved from https://www.csoonline.com/article/3209653/disaster-recovery/7-things-your-it-disaster-recovery-plan-should-cover.html
- Messer. (2012). Using protocol analyzers - CompTIA Network+ N10-005: 4.3 [Video]. Retrieved from https://www.youtube.com/watch?v=w4P2qqCdWXw
- Messer. (2015). Using protocol analyzers – CompTIA Network+ N10-006 - 2.1 [Video]. Retrieved from https://www.youtube.com/watch?v=UQ1NKip5tcc
- 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
- OWASP.org. (2016). Security by design principles. Retrieved from https://www.owasp.org/index.php/Security_by_Design_Principles
- 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
- Simplilearn. (2018). Key roles & responsibilities of IT security professionals. Retrieved from https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article
- 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

- Yang, C. (2018). Global information assurance certification paper: Operating system security and secure operating systems [PDF]. Retrieved from https://www.giac.org/paper/gsec/2776/operating-system-security-secure-operating-systems/104723

Suggested

Optional

Unit 1 >> Principles of 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 with those policies. 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 strategies of the organization.

In this unit, you explore the importance of security approaches in an organization and implement technical policies that can have a great effect on the overall security posture of an organization. You will explore a variety of elements which will establish a thorough foundation for the information systems profession and industry. Moreover, the domains of a typical IT Infrastructure will be examined as well as common network tools to perform analysis and evaluation of exposures on the network.

One of the important parts of securing a network is being able to perform network reconnaissance and probing. In the unit assignment, you will complete a lab called *Performing Reconnaissance and Probing Using Common Tools.*

Learning Activities

u01s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 1, "Information Systems Security," pages 2–42.

Use the Capella University Library to read the following:

- Kalsi, T. (2017). Nmap: Network security scans. *Linux Format*, (219), 76–77.
  - The article examines how to use the network scanner called Nmap.
- Bou-Harb, E., Debbabi, M., & Assi, C. (2014). On fingerprinting probing activities. *Computers & Security, 43*, 35–48.
  - The paper discusses new approaches to the fingerprint propping activity.
- Parkyn, J. (2018). Wireless network scanning tools. *Web User*, (443), 48–49.
  - This article discusses how to user common network scanning tools effectively.
- Singh, G., Goyal, S., & Agarwal, R. (2015). Intrusion detection using network monitoring tools. *IUP Journal of Computer Sciences, 9*(4), 46–58.
  - The paper introduces basic approaches for using instruction detection tools.
- Tsoukalos, M. (2016). Wireshark: Analyse traffic. *Linux Format*, (218), 80–83.
  - In this article, the benefits and features of Wireshark are provided with an emphasis on traffic analysis.
- Jingguo, W., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly, 39*(1), 91–97.
  - This study investigates the risk of insider threats associated with different applications within a financial institution.
- Bahtiyar, Ş. (2016). Anatomy of targeted attacks with smart malware. *Security & Communication Networks, 9*(18), 6215–6226.
  - The article helps in the examination of targeted attacks on PCs by smart malware.

Use the Internet the watch the following videos.

- Messer. (2012). Using protocol analyzers - CompTIA Network+ N10-005: 4.3 [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=w4P2qqCdWXw
  - Introduces principles of protocol analysis.
- Alexander, A. (2015). Wireshark Tutorial for beginners [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=TkCSr30UojM
  - Demonstrates the fundamentals of using Wireshark.

u01s1 - Learning Components

- Explain applications for Wireshark and NetWitness.
- Explain network areas that are scanned by WireShark and NetWitness.
- Identify elements of typical probe and reconnaissance results.
- Explain what constitutes secure log on credentials.
- Interpret probe results.

u01s2 - Kaltura Media Preparation

The Unit 10 assignment requires you to record audio for a presentation. You **may choose** to use Kaltura Media or other software. Refer to the Using Kaltura [PDF] tutorial for directions on recording and submitting your recording in the courseroom using Kaltura.

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 DisabilityServices@Capella.edu to request accommodations.

u01d1 - Reconnaissance and Probing Tools

There are many tools used for network reconnaissance and probing. Among them are WireShark, NetWitness, Cryptool, and Tripwire. Research one of these tools on the Internet and discuss the following:

- How does it work?
- What systems does it examine?
- What types of threats is it designed to detect?
- How should it be used to keep a network safe?

As with most discussions in this course, it is recommended that you post your initial post early in the week to allow time for your peers to respond.

Response Guidelines

Early in the unit, read your peers' posts and provide feedback to at least two of them. It is highly recommended that you extend the dialog further. This will provide you with more opportunity for in-depth interaction with your peers and the instructor. Responding over multiple days will also help in stimulating a lively discussion.

Course Resources
Graduate Discussion Participation Scoring Guide

- Explain applications for Wireshark and NetWitness.

u01v1 - Lab: Performing Reconnaissance and Probing Using Common Tools

Read this unit's assignment completely before completing this lab. The assignment's lab-related questions may be more easily answered if you consider them at the time you take the lab.

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

Directions

Note: Not all of the directions within the lab are required for this assignment. You are only responsible for completing the lab and saving the specified screenshots.

Complete Section 1 of the Lab.

To demonstrate your understanding of core concepts and procedures used in the lab, you will be required to submit a Word document with the following information in this unit's assignment:

- Specified lab screenshots (in order taken and appropriately titled with step number).
- Answers to questions found in the unit assignment.

Jones & Bartlett Learning Technical Support

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

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

u01a1 - 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 activities are detected in a timely fashion. This action is accomplished using intrusion detection and prevention systems (IDS or IPS). In order to increase security governance and posture, many organizations may also perform penetration and ethical hacking testing, which can be useful in detecting security vulnerabilities before others.

Directions

Address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Compare and contrast the uses of NetWitness Investigator and Wireshark used in the lab. Why would a network administrator use Wireshark and NetWitness Investigator together?
2. Interpret the results of the Wireshark and NetWitness scans performed in the lab. Describe the area of network vulnerability found in each scan.
3. Describe the security risk associated with the vulnerability you discovered.
4. Suggest a security control that you would use to address the vulnerability and explain why it is appropriate.
5. Explain in detail the results returned from the Zenmap reconnaissance.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Unit 2 >> Networking Monitoring and Management

Introduction

There are many network monitoring tools and techniques that are available to network administrators that support this line of work. Administrators rely on scanning tools to perform network traffic analysis. For example, they can aid in packet capture and real-time stream analysis to troubleshoot complex issues such as network and application performance degradations. This unit explores tools used to detect irregularities on the network.

In this unit, you discuss hacking and complete a lab called *Performing Packet Capture and Traffic Analysis.*

Learning Activities

u02s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 3, "Malicious Attacks, Threats, and Vulnerabilities," pages 72–108.

Use the Capella University Library to read the following.

- Hartley, R. D. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management, 24*(4), 95–104.
    - This article discusses a panoramic approach to ethical hacking.
- Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165–176.
    - This study offers an interesting and fascinating perspective to crime over the Internet.

Use the Internet to watch the following video:

- Messer. (2015). Using protocol analyzers - CompTIA Network+ N10-006 - 2.1 [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=UQ1NKip5tcc
    - In this video, Professor Messer discusses the application of common network scanners, also known as protocol analyzers.

u02s1 - Learning Components

- Understand how Wireshark works.
- Explain packet capture control.

u02d1 - Hacking: Black Hat vs. White Hat

The hacking process consists of the following five steps:

- Footprinting.
- Scanning and vulnerability assessment.
- Enumeration.
- Exploitation (the actual attacks).
- Post-attack activities (including covering tracks and planting backdoors).

Black-hat hackers operate covertly, but ethical hackers (white-hat hackers) add an additional step at the beginning; they obtain written authorization from the target, their client, to perform the scanning and vulnerability assessment on a live production network. The differences between the ethical hacker and an attacker are written permission, complete transparency, and professional accountability.

- Discuss what factors go into deciding while hiring a black-hat hacker vs. a white-hat hacker?
- Explain why organizations will hire a convicted hacker (black-hat). Include in the discussion how you would prioritize your justifications. Provide support for your position.

As with most discussions in this course, it is recommended that you post your initial post early in the unit to allow time for your peers to respond.

Response Guidelines

Early in the unit, read your peers' posts and provide feedback to at least two of them. It is highly recommended that you extend the dialog further. This will provide you with more opportunity for in-depth interaction with your peers and the instructor. Responding over multiple days will also help in stimulating a lively discussion.

Course Resources
Graduate Discussion Participation Scoring Guide

u02d1 - Learning Components

- Explain Black and White Hat hacking.

u02v1 - Lab: Performing Packet Capture and Traffic Analysis

Read this unit's assignment completely before completing this lab. The assignment's lab-related questions may be more easily answered if you consider them at the time you take the lab.

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

Directions

Note: Not all of the directions within the lab are required for this assignment. You are only responsible for completing the lab and saving the specified screenshots.

Complete Section 1 of the Lab.

To demonstrate your understanding of core concepts and procedures used in the lab, you will be required to submit a Word document with the following information in this unit's assignment:

- Specified lab screenshots (in order taken and appropriately titled with step number).
- Answers to questions found in the unit assignment.

Jones & Bartlett Learning Technical Support

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

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

u02a1 - 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.

Directions

Address each of the following in the Word document that contains your screenshots. Clearly label each section.

1. The main screen of Wireshark includes details about the current capture configuration. From this screen, analysts can select recently used filters from the drop-down menu or type a custom filter command to quickly sort the captured data. Select and state the type of data that you would like to analyze and a possible reason for you wanting to analyze it, choose an appropriate filter (or write a custom filter command), and describe the results that are returned.
2. Promiscuous mode allows Wireshark to capture packets destined to any host on the same subnet or virtual LAN (VLAN). Without this option selected, Wireshark would only capture packets to and from the TargetWindows02 machine. Explain how promiscuous mode acts as a security control for capturing network packets.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Unit 3 >> Secure Components of Network Devices

Introduction

This unit explores the functionality and options available with common network devices. Most network devices have multiple objectives and functions, which will create a huge challenge for the Operations and Administration team. The overall objective of a modern data and communications network is to provide functionality that supports business objectives. The secondary interest to security administrators involves creating a balance between the desired availability of the users of the network and the need to ensure that availability happens in the most secure means possible. You will explore how the Operations and Administration team must focus on these dual objectives to achieve the proper balance.

In this unit's activities, you discuss protecting CIA and complete a lab called *Performing a Vulnerability Assessment.*

Learning Activities

u03s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 6, "Security Operations and Administration," pages 181–212.

Use the Capella University Library to read the following:

- Singh, G., Kaur, R., & Kaur, A. (2016). An approach to detect vulnerabilities in web-based applications. *International Journal of Advanced Research in Computer Science, 7*(1).
    - This article examines web applications and the ever-changing web application security needs.
- Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P., & Mauro Madeira, E. R. (2015). Virtual network security: Threats, countermeasures, and challenges. *Journal of Internet Services and Applications, 6*(1), 1–19.
    - The article talks about the creation of network infrastructures.
- Joshi, C., & Singh, U. K. (2017). Information security risks management framework–A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128–137.
    - This paper analyzed the security threats specifically evolve in a University's network.
- Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal Of Business Continuity & Emergency Planning, 11*(2), 163–173.
    - The paper discusses why critical infrastructure is crucial to the functionality of an organization.

- Identify ways scan processes effect a target host.
- Understand Ports/Hosts and Host information.
- Understand how Nmap and SYN scans work.

u03d1 - Protecting CIA

Confidentiality, *integrity*, and *availability*, also known as the CIA triad, is a model designed to guide policies for information security within an organization. Computer security is accomplished using many different systems, but the fundamental concepts are all rooted in the CIA triad. Confidentiality is preventing the disclosure of secure information to unauthorized individuals or systems. Integrity is maintaining and assuring the accuracy of data over its life-cycle. For information to be useful, it must be available when needed; thus, the need for availability. Everything in network operations and administration centers around CIA. The reason is that it is charged with all the network management functions that provide network fault indication, performance information, and data and diagnosis functions.

- Identify a security threat to a component on your network to CIA that interests you. Explain how it is commonly detected and defended by the department in charge of operations and administration.

Response Guidelines

Respond to at least two other learners and share what you found most informative about their posts.

Course Resources
Graduate Discussion Participation Scoring Guide

u03d1 - Learning Components

- Describe elements of the NIST National Vulnerability Database.

u03v1 - Lab: Performing a Vulnerability Assessment

Read this unit's assignment completely before completing this lab. The assignment’s lab-related questions may be more easily answered if you consider them at the time you take the lab.

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

Directions

Note: Not all of the directions within the lab are required for this assignment. You are only responsible for completing the lab and saving the specified screenshots.

Complete Section 1 of the Lab.

To demonstrate your understanding of core concepts and procedures used in the lab, you will be required to submit a Word document with the following information in this unit's assignment:

- Specified lab screenshots (in order taken and appropriately titled with step number).
- Answers to questions found in the unit assignment.

Jones & Bartlett Learning Technical Support

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

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

u03a1 - 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 the vulnerabilities associated with those assets. One of the common ways to do this is by performing vulnerability assessments on our assets and developing strategies for managing the risk that results from those vulnerabilities.

Directions

Address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Explain which scan process is more intrusive to the target host, SYN or TCP.
2. Explain the information provided in the Ports or Hosts and Host Details tab for each host in the Nmap scan in the lab. What does it tell you?
3. Compare Nmap and SYN scans. What are the differences and similarities?
4. Explain the importance to data security of the National Vulnerability Database established by NIST.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Unit 4 >> Network Design and Management Roles and Responsibilities

Introduction

Unit 4 focuses on secure network design and effective management of installed networks. The network that supports each organization is unique and requires careful assessment of the specific characteristics unique to that implementation. The factors considered go beyond those that impact the initial selection and installation. The plans of the organization and the ongoing impacts of that design on the ability to effectively manage the network are also of critical importance. The size of the organization, the number of locations, the number of transactions, and the level of sensitivity of the data that will be streaming across the network are all examples of critical factors to consider when designing a secure network.

In this unit's activities, you analyze a network and identify the security risks posed to it.

Learning Activities

u04s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 2, "The Internet of Things Is Changing How We Live," pages 47–69.

Use the Capella University Library to read the following:

- Armour, M. (2015). Talking about a (business continuity) revolution: Why best practices are wrong and possible solutions for getting them right. *Journal Of Business Continuity & Emergency Planning*, *9*(2), 103-111.
- Ayub, K., & Zagurskis, V. (2015). Technology implications of UWB on wireless sensor network-A detailed survey. *International Journal of Communication Networks and Information Security, 7*(3), 147-161.
    - This survey identifies core obstacles of wireless sensor network when UWB (Ultra-Wideband) is used at the layer.

Use the Internet to read the following:

- Simplilearn. (2018). Key roles & responsibilities of IT security professionals. Retrieved from https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article
    - This article discuses a few of the primary roles for IT security professionals.

u04s1 - Learning Components

- Describe security exposures commonly faced by networks.
- Ability to read a network diagram.
- Describe the operation of network security hardware mechanisms.
- Understand multiple methods of vulnerability testing.

u04d1 - Evaluating Exposures and Risks

When analyzing network exposures and risks, it is important to consider the following:

- Identifying and prioritizing network threats.
- Analyzing router and Wi-Fi passwords for vulnerabilities.
- Reviewing the organization’s network strength against common attacks including Distributed Denial of Service (DDoS), Man-in-the-Middle attack (MITM), and Network Intrusion.
- Analyzing routers, switches, and computers for device security weaknesses.
- Determining if firewalls are correctly configured and located.

Discuss some additional things that you would consider when preparing to analyze network risks and why they are important.

Response Guidelines

Respond to at least two other learners and expand on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Graduate Discussion Participation Scoring Guide

u04d1 - Learning Components

- Describe security exposures commonly faced by networks.

u04a1 - Scenario: Analyze a Network's Security Risk

Overview

Analyzing a network's security risks is one of the first steps in creating a secure network. All the hard work a company does to generate traffic and promote itself online can go up in flames if it is not protected from network security threats. The company may not even be aware of a problem until it is too late. Some of the most common network security risks are:

- Computer viruses.
- Software vulnerabilities.
- Hackers.
- Employee breaches.

In this assignment, you analyze a network and identify the security risks posed to it.

Preparation

Download and examine the Network Configuration document found in the assignment Resources. Use the information in it to complete this assignment.

Directions

Consider the network configuration and create a 2–3 page Word document in which you will perform the following activities:

- Discuss the significant network risks that exist for any three of the following:
  - Confidentiality.
  - Integrity.
  - Availability.
  - Identification.
  - Authentication.
  - Authorization.
  - Accountability.
- Assess the network's ability to mitigate your identified exposures. Make sure to identify specific areas of weakness that include a discussion of hardware and software.
- Describe a process or procedure for performing vulnerability testing that effectively assesses this network's security weaknesses.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).

- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Course Resources
Network Configuration [PDF]

Unit 5 >> Application of Security Principles

Introduction

One approach to protecting CIA is the use layers of defense. This tactic describes the concept of attaching multiple mitigating security controls (layers) to protect assets and systems. The challenge of keeping networks and computers secure has never been greater. Several current events pertaining to data security, illustrate why security is becoming increasingly difficult. To create a more precise approach to information security, security professionals should consider the goals of security principles and how they can be accomplished.

In this unit's activities, you discuss OWASP security principles and complete a lab called *Eliminating Threats with a Layered Security Approach*.

Learning Activities

u05s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 11, "Malicious Code and Activity," pages 352–393.

Use the Capella University Library to read the following:

- Araújo, J. D., Rodrigues, D. d. A., de Melo, L. S., & Abdelouahab, Z. (2015). EICIDS-elastic and internal cloud-based detection system. *International Journal of Communication Networks and Information Security, 7*(1), 34–49.
    - This paper discusses the vulnerabilities when using cloud-based detection systems.
- El uahhabi, Z., & El bakkali, H. (2016). Calculating and evaluating trustworthiness of certification authority. *International Journal of Communication Networks and Information Security, 8*(3), 136–146.

- This article evaluates the trustworthiness of public key infrastructure trust model and certificate authorities.

Use the Internet to read the following:

- Hnatiw, A. (2017). A guide to implementing the top ten security principles for business. Retrieved from https://blog.securitycompass.com/are-you-following-the-top-ten-security-principles-for-business-9c28cf9ccd50/
  - This article discusses the most critical measures for ten common security principles.

u05s1 - Learning Components

- Explain fundamentals of how malware works.
- Explain basic firewall settings.

u05d1 - OWASP Security Principles

Pick two of the security principles listed on the OWASP website and discuss how they impact CIA.

Response Guidelines

Read the posts of your peers and respond to at least two of them. Expand on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Graduate Discussion Participation Scoring Guide
Security by Design Principles

u05d1 - Learning Components

- Explain the basics of CIA and risks facing it.

u05v1 - Lab: Eliminating Threats with a Layered Security Approach

Read this unit's assignment completely before completing this lab. The assignment's lab-related questions may be more easily answered if you consider them at the time you take the lab.

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

Directions

Note: Not all of the directions within the lab are required for this assignment. You are only responsible for completing the lab and saving the specified screenshots.

Complete Section 1 of the Lab.

To demonstrate your understanding of core concepts and procedures used in the lab, you will be required to submit a Word document with the following information in this unit's assignment:

- Specified lab screenshots (in order taken and appropriately titled with step number).
- Answers to questions found in the unit assignment.

Jones & Bartlett Learning Technical Support

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

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

u05a1 - Eliminating Threats with a Layered Security Approach

Overview

Security controls eventually fail. This is what makes layered security defenses so important. When a single control does indeed fail, there are other controls in place that will together help mitigate the risk of the failed control.

Directions

Address each of the following in the Word document that contains your screenshots. Clearly label each section.

1. Malware consists of unwanted programs like Trojans and viruses. Signs of malware include degraded system performance, unusual services and network traffic, altered or removed system logs, missing or inactive anti-

virus, and any number of application anomalies. Trojans and viruses impact all three tenets of information systems security.
    - Identify and describe three techniques used in the lab to defend against malware. Describe some advantages and disadvantages of each.

2. Enabled on the network and properly configured, a firewall can block outside sources from being able to insert malware and viruses. By default, the Windows Firewall disables several important services like File Transfer Protocol (FTP) and Internet Control Message Protocol (ICMP), both of which use the Ping command.
    - Explain why enabling these default settings is significant to network security. Elaborate on what can happen if they are left disabled.

3. Pick one of the following defense layers and provide descriptions (including how they work) of two controls or countermeasures that can be effectively used within it.
    - Perimeter.
    - Network.
    - Host.
    - Application.
    - Data.
    - Physical.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Unit 6 >> Incident Response and Contingency Planning

Introduction

This unit covers the concepts of incident response and contingency planning. The percentage of businesses that survive and are still in business five years after a major data incident or disaster is very low. The reality is that planning for events that may never happen often does not get a high priority in many organizations, despite these grim figures of the impact on those businesses for failure to plan. Information security professionals are not always able to influence enterprise-level planning; however, prudent professionals examine the environment and include their own planning for how security can be maintained to address risk, response, and recovery.

Most organizations do not have trained in-house forensics professionals, so they are unprepared when an incident occurs that requires the collection of evidence. An effective security professional will have initiated activity toward identifying resources, creating procedures, and having the framework for a response to a critical incident.

In this unit's activities, you discuss disaster recovery and complete a lab called *Implementing a Business Continuity Plan*.

Learning Activities

u06s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 4, "The Drivers of the Information Security Business," pages 112–131.
- Chapter 8, "Risk, Response, and Recovery," pages 215–285.

Use the Capella University Library to read the following:

- Baham, C., Hirschheim, R., Calderon, A. A., & Kisekka, V. (2017). An agile methodology for the disaster recovery of information systems under catastrophic scenarios. *Journal Of Management Information System, 34*(3), 633–663.
    - The article explores the use of an agile methodology for improving the recovery of complex systems under catastrophic scenarios.
- Tao, L., Ning, X., Chunqiu, Z., Wubai, Z., Li, Z., Yexi, J., & Iyengar, S. S. (2017). Data-driven techniques in disaster information management. *ACM Computing Surveys*, *50*(1), 1–45.
    - This article provides reasons for improving disaster management and recovery techniques.

u06s1 - Learning Components

- Explain elements of a business continuity plan.
- Understand basic Windows OS Server features.
- Explain the mechanism for daily server backups.
- Explain the importance and mechanisms for serer backups.
- Read backup command line code.

u06d1 - Disaster Recovery Program

Read Martin's article (linked in the resources) on effective disaster recovery planning, or research other resources on similar topic.

Discuss what you believe are the most significant elements to an effective disaster recovery plan. Provide details to reinforce your opinions.

Response Guidelines

Read the posts of your peers and respond to at least two of them. Expand on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Graduate Discussion Participation Scoring Guide
7 Things Your IT Disaster Recovery Plan Should Cover.

u06d1 - Learning Components

- Explain elements of a business continuity plan.

u06v1 - Lab: Implementing a Business Continuity Plan

Read this unit's assignment completely before completing this lab. The assignment's lab-related questions may be more easily answered if you consider them at the time you take the lab.

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

Directions

Note: Not all of the directions within the lab are required for this assignment. You are only responsible for completing the lab and saving the specified screenshots.

Complete Section 1 of the Lab.

To demonstrate your understanding of core concepts and procedures used in the lab, you will be required to submit a Word document with the following information in this unit's assignment:

- Specified lab screenshots (in order taken and appropriately titled with step number).
- Answers to questions found in the unit assignment.

Jones & Bartlett Learning Technical Support

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

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

u06a1 - 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.

Directions

Address each of the following in the Word document that contains your screenshots. Clearly label each section.

1. During the installation of the Windows Server Operating System you are instructed: “On the Features page, click the Client for NFS checkbox to enable the computer to access files on UNIX-based NFS servers and click the Windows Server Backup checkbox to allow you to backup and recovery data, then click Next to continue.”
    - Explain the rationale for making these selections.
2. Windows Server Backup is used to make a daily backup of System State. This same process is used for Active Directory servers. (Active Directory contains the users, groups, distribution lists, and organizational units used in the domain.)
    - Explain the issues or concerns to consider when developing a strategy for the daily backup.
3. Originally used in the UNIX operating system, a Network File System is used to make remote folders appear as part of the local file system on Linux and Windows systems.
    - Describe the reason for configuring redundant web servers (www1 and www2) to use a Network File System (NFS) on a third storage server for web content.
4.

In the lab with the same name as this assignment, you are provided with the following syntax:

```
cd \
    cd www
    xcopy * c:\backup /i /y
```

Interpret or translate the code. Explain in detail what the code will do for the user.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Unit 7 >> Selection, Installation, and Secure Configuration of Operating Systems

Introduction

Microsoft Windows is the world's most used consumer operating system. Its popularity also makes it a target for malware which exploits vulnerabilities and insecure user practices on the Windows operating system targets vulnerabilities and insecure user practices on the Windows operating system.

Many people may not even know that there are alternatives to Windows. There are two chief operating system alternatives. One is Mac (Mac OS X) and the other is the UNIX-like family of operating systems, of which GNU/Linux is the most well-known. These UNIX-like operating systems are free and open source; these are distributed freely and with source code that can be independently audited or modified by anyone.

In this unit's activities, you discuss how to secure an OS and complete an assignment on how to secure a network for the Network Configuration you considered in Unit 4.

Course Resources
Network Configuration [PDF]

Learning Activities

u07s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 5, "Access Controls," pages 136–177.

Use the Capella University Library to read the following:

- Wu, Z., Cai, M., Liang, S., & Zhang, J. (2014). An approach for prevention of MitM attack based on rogue AP in wireless network. *Sensors & Transducers, 183*(12), 162–171.
  - Discusses a dynamic password technology named Two-way Dynamic Authentication Technology (TDAT).
- Madhavapeddy, A., & Scott, D. J. (2014). Unikernels: The rise of the virtual library operating system. *Communications Of The ACM, 57*(1), 61–69.
  - The article provides information on the virtual operating systems in cloud computing.

u07s1 - Learning Components

- Explain common methods for improving network security.
- Identify network controls and how they are used to secure networks.

u07d1 - Securing the Operating Systems

Many operating system (regardless of vendor) intrusions could be prevented by performing some of the following actions:

1. Creating a white-list of approved applications.
2. Patching third-party applications and OS vulnerabilities.
3. Restricting admin privileges to users who need them.
4. Creating a defense-in-depth configuration plan for software, hardware, resources, et cetera.

Discuss three more actions that are effective for mitigating cyber-attacks on an operating system. Provide details and explanations to support your learning points.

Response Guidelines

Read the posts of your peers and respond to at least two of them. Expand on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources

Graduate Discussion Participation Scoring Guide

u07d1 - Learning Components

- Identify OS vulnerabilities.

u07a1 - Scenario: Securing a Network

Overview

An exposure is a weak spot in your network that might be exploited by a security threat. Risks are the potential consequences and impacts of unaddressed exposures. For example, failing to do Windows Updates on your Web server creates a vulnerability. Some of the risks associated with that vulnerability include loss of data, hours or days of site downtime, and the staff time needed to rebuild a server after it has been compromised. Securing a network entails minimizing risk.

In this assignment, you explain how to address the network security exposures that you identified in the unit 4 assignment.

Preparation

Review the Network Configuration document found in the assignment Resources as needed.

Directions

Do the following:

1. Explain how you would address **two** of the exposures you identified in the unit 4 assignment to improve the network's security.
2. Explain which of the following controls that you believe would be one of the most important in addressing the exposures inherent in the network in the scenario. Why?
    - Encryption.
    - Firewall.
    - Access control lists.
    - VPNs.
    - Login or accountability.
    - Anti-Virus.
    - Protocols.
    - IPS.
    - IDS.
3. Select two of the controls from the list above and explain their relative advantages and disadvantages.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Course Resources

Network Configuration [PDF]

Unit 8 >> Operating System and Application Patching

Introduction

Unit 8 focuses on patch management. Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Many organizations have largely operationalized their patch management, making it more of a core IT function than a part of security. However, it is still important for all organizations to carefully consider patch management in the context of security because it is important to achieving and maintaining sound security.

There are several challenges that complicate patch management. Organizations that do not overcome these challenges will be unable to patch systems effectively and efficiently, leading to compromises that are easily preventable. Currently, software distribution and patches are done digitally with the help of digital signatures, digital certificates, hashing, steganography, encryption, proof of origin, and non-repudiation. In other words, cryptography. Also, the OS for a variety of mobile platforms is a major consideration of operating systems and patches.

In the unit activities, you discuss system patching and data backups and complete a lab called *System Management and Backups.*

Learning Activities

u08s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 9, "Cryptography," pages 288–323.

Use the Capella University Library to read the following:

- Barthe, G., Grégoire, B., Heraud, S., Olmedo, F., & Zanella-Béguelin, S. (2016). Verified indifferentiable hashing into elliptic curves. *Journal of Computer Security, 21*(6), 881–917.
    - The paper discusses encryption in small mobile devices using elliptic curve technology.
- Bhutta, M. N., Cruickshank, H., & Sun, Z. (2016). An efficient, scalable key transport scheme (ESKTS) for Delay/Disruption tolerant networks. *Wireless Networks, 20*(6), 1597–1609.
    - The article discusses the need to address secure transportation of secret keys is presented to the reader and examines ESKTS in detail.
- Das, A. (2015). A secure and efficient user anonymity-Preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. *Wireless Personal Communications, 82*(3), 1377–1404.
    - Through this article the authors provide a diversified perspective to emphasizing three-factor vs. two-authentication protocols.
- Jaheel, H. L., Zou, B., & Jaheel, A. L. (2015). Design and implementation steganography system by using visible image. *International Journal On Smart Sensing & Intelligent Systems, 8*(2), 1011–1030.
    - This article is an intriguing examination of steganography is offered in this paper.
- Phan, R. C. -W. (2011). Non-repudiable authentication and billing architecture for wireless mesh networks. *Wireless Networks, 17*(4), 1055–1061.
    - The article discusses authentication that is non-repudiated over a wireless network.

Use the Internet to read the following:

- Yang, C. (2018). Global information assurance certification paper: Operating system security and secure operating systems [PDF]. Retrieved from https://www.giac.org/paper/gsec/2776/operating-system-security-secure-operating-systems/104723
    - This paper examines the security of operating systems Windows and Unix and its overall security on applications and services.

u08s1 - Learning Components

- Identify SQL injection attack prevention controls.
- Explain the fundamentals of SQL injections attacks.
- Explain basic hacking techniques.
- Describe vulnerabilities associated with clear text passwords.

u08d1 - Security and Patch Management

Patch management is the process of handling all the updates of components within an organization's information system. Targets include routers, firewalls, servers, operating systems, anti-viruses, along with many others. Patch is a piece of code that must be installed; therefore, security concerns are present. Reflect on your experience and research on this topic.

Discuss a security best practice patch management. Support your ideas with references from academic or other professional resources.

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide

u08d1 - Learning Components

- Identify patch management best practices.

u08v1 - Lab: Performing a Website and Database Attack by Exploiting Identified Vulnerabilities

Read this unit's assignment completely before completing this lab. The assignment's lab-related questions may be more easily answered if you consider them at the time you take the lab.

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

Directions

Note: Not all of the directions within the lab are required for this assignment. You are only responsible for completing the lab and saving the specified screenshots.

Complete Section 1 of the Lab.

To demonstrate your understanding of core concepts and procedures used in the lab, you will be required to submit a Word document with the following information in this unit's assignment:

- Specified lab screenshots (in order taken and appropriately titled with step number).
- Answers to questions found in the unit assignment.

Jones & Bartlett Learning Technical Support

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

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

u08a1 - Performing a Website and Database Attack by Exploiting Identified Vulnerabilities

Overview

The Operating System (OS) is the most important component of our computer system. Performing installs, maintenance, and patches can pose a variety of challenges to secure. For example, with the reliance on software-as-a-service (SaaS) providers increases in organizations, it is becoming more and more important for SaaS providers to create secure products and services. One process that can help in these efforts is to competently secure and test OS applications with security in mind. Additionally, it is relevant for security testers to understand certain hacking techniques that could be used by hackers in order to ensure OS products and services are not prone to certain attacks, such as cross-site scripting and SQL injection. In the lab, you will perform an activity to execute attacks that can be handled by the operating system level.

Directions

Address each of the following in the Word document that contains your screenshots. Clearly label each section.

1. The scripts in this lab are all typed in clear text to make it easier for you to understand the process. Often hackers will use hexadecimal character strings instead of clear text to make the scripts harder to detect.
    - Explain the controls provided in the lab that can be used to avoid issues with clear text passwords.
2. Poorly designed or improperly secured web forms can be exploited to output passwords, credit card information, and many kinds of other data. In this lab, you inserted a series of SQL statements into a web form to find and then exploit an SQL injection vulnerability.
    - Explain, in detail, how SQL Injection attacks are used to extract privacy data elements out of a database.
    - Describe a control used to prevent SQL Injection attacks.
3. In this lab, you are asked to ***Type 'UNION SELECT 'test', '123' INTO OUTFILE 'test1.txt and click Submit.*** Together with the information you gathered in earlier tests, you now have a user with elevated permissions, user IDs, passwords, and the table structure where all this data is being held—in other words, an injectable database.

- Analyze the complete lab experience and explain how the hacker can accomplish this type of breach.

4. Today, nearly all data is stored in a database and this can create issues for data security. Identify and explain how a common attack aimed specifically at databases works.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Unit 9 >> Security Policy

Introduction

Information Security Policy (ISP) is a set of rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. Furthermore, a security professional should make sure that the ISP has an equal institutional gravity as other policies enacted within the corporation. In cases where an organization has sizeable structure, policies may vary and therefore be separated to define the dealings in the intended subset of this organization.

ISP is deemed to safeguard three main objectives:

- Confidentiality - Data and information assets must be confined to people authorized to access and not be disclosed to others.
- Integrity - Keeping the data intact, complete and accurate, and IT systems operational.
- Availability - Indicating that the information or system is at disposal of authorized users when needed.

Implementing technical policies that align with the information security plans and “paper” policies in organizations is critical to the adoption, adherence, and compliance with 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. To compound this task, organizations may have Information Security Standards to consider. And on top of that, your organization may have to deal with regulations and compliance laws.

In the unit activities, you discuss network monitoring tools and complete a lab called *Implementing an Information Systems Security Policy*.

Learning Activities

u09s1 - Studies

Readings

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 12, "Information Security Standards," pages 396–410.
- Chapter 15, "U.S. Compliance Laws," pages 452–487.

Use the Capella University Library to read the following:

- Denton, P. D., & Maatgi, M. K. (2016). The development of a work environment framework for ISO 9000 standard success. *The International Journal of Quality & Reliability Management, 33*(2), 231–245.
  - The article discusses the ISP 9000 standard.
- Rooney, J. J. (2017). A holistic approach to identify, understand, and mitigate risk. *The Journal for Quality and Participation, 40*(1), 39–40.
  - In this article, the author details the issues pertaining to changes in a business environment and impact it has on regulations.

Use the Internet to read the following:

- 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
  - The document provides 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 document is a policy template for workstation security in a healthcare organization.
- 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
  - This is 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

Watch the following Skillsoft video:

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

u09d1 - 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

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

Course Resources
Graduate Discussion Participation Scoring Guide

u09v1 - Lab: Implementing an Information Systems Security Policy

Read this unit's assignment completely before completing this lab. The assignment's lab-related questions may be more easily answered if you consider them at the time you take the lab.

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

Directions

Note: Not all of the directions within the lab are required for this assignment. You are only responsible for completing the lab and saving the specified screenshots.

Complete Section 1 of the Lab.

To demonstrate your understanding of core concepts and procedures used in the lab, you will be required to submit a Word document with the following information in this unit's assignment:

- Specified lab screenshots (in order taken and appropriately titled with step number).
- Answers to questions found in the unit assignment.

Jones & Bartlett Learning Technical Support

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

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

u09a1 - 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.

Directions

Part 1

Address each of the following in the Word document that contains your screenshots. Clearly label each section.

1. In this lab, you implemented an organization’s password policy using Group Policy. Group Policy uses a layered approach to apply policy at the local server, domain, and sub-domain (organizational unit) level. Policies at the organizational unit level take precedence over domain and local policies.
    - Explain why the sequence is in this order.
2. In this lab, you were tasked with hardening the password policies. Identify a password policy and explain why it is significant for password security.

Part 2

Follow the directions found in the Laskondo Healthcare Scenario linked in the Resources. Add your work to your assignment document.

Make sure to read the Background and the Technical Details sections before you begin writing. Take note that the assignment requires you to draft a 2-page security policy for one of the areas provided in the Laskondo case. Reference the course content and readings to demonstrate critical thinking. Produce a security policy that is professional and relevant to the needs of Laskondo Healthcare.

Submission Instructions

- Submit your assignment in a Word document with well-labeled responses.
- Length: 2–3 double-spaced pages (not including screenshots).
- Format and Style: Current APA standards.
- Font: 12 point Times New Roman.

Course Resources

Laskondo Healthcare Scenario [PDF]

Unit 10 >> Communication and Data Network Architecture?

Introduction

The tools and technologies that are available to construct and secure a modern data and communications network have expanded and provide network and security administrators with a wide array of choices. The number of choices allows administrators to better customize a solution that fits within an environment. It also requires administrators to spend more time researching and selecting from among those solutions. This unit explores these tools and technologies and how they impact the overall design and architecture of a secure enterprise network using both wired and wireless technologies.

In this unit's assignment, you create a presentation summarizing your work regarding the network configuration that you worked on in earlier units and consider a security policy that would help to protect the network.

Learning Activities

u10s1 - Studies

Reading

Use *Fundamentals of Information Systems Security* to read the following:

- Chapter 10, "Networks and Telecommunications," pages 326–351.

Use the Capella University Library to read the following:

- Masmoudi, K., & Afifi, H. (2008). Building identity-based security associations for provider-provisioned virtual private networks. *Telecommunication Systems, 39*(3-4), 215–222.
    - This article presents an adaptation of the Internet Key Exchange (IKEv2) protocol to the context of dynamic tunneling in personal networks.
- Marion, T. J., Reid, M., Hultink, E. J., & Barczak, G. (2016). The influence of collaborative IT tools on NPD. *Research Technology Management, 59*(2), 47–53.
    - The article suggests that NPD managers should encourage the use of new forms of communication and collaboration and should embolden and empower the migration toward these collaborative tools.

u10s1 - Learning Components

- Describe the functions of basic security policies.
- Identify common security policies.
- Identify methods for monitoring networks.

u10s2 - Kaltura Media

In preparation for creating the audio recordings required for this unit's assignment, do the following **only if you plan to use Kaltura for your presentation**:

- If you have not already done so, set up and test 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 [PDF] 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 DisabilityServices@Capella.edu to request accommodations.

u10d1 - Communication and Social Networks

Communications networks and architectures have produced capabilities and applications that have profoundly impacted our lives. For example, social network tools like Facebook have changed the way we interact in our personal lives and are in the process of transforming our professional lives as well.

As communications networks play a more significant role in how business gets done, they become more attractive targets.

Share your thoughts and reflection on the threats or risks that enterprises must consider when developing policies for social networks.

Response Guidelines

Read the posts of your peers and respond to at least two of them. Expand on the concepts covered in their initial posts. The quantity and quality of your posts will determine the value of the group's learning experience. Provide a substantive and appropriate response.

Course Resources
Graduate Discussion Participation Scoring Guide

u10a1 - Security Findings, Recommendations and Policy Presentation

Overview

Networks exposures face new risks every day, which makes continuous network monitoring critical. Policies governing areas like this are equally important. Explaining this to stakeholders is increasingly important to make sure security issues are well understood.

In this assignment, you create a presentation that summarizes your earlier work regarding the security issues and recommendations for the Atlas Financial Company network. The presentation should also recommend policies intended to assure future network security.

Preparation

Follow the steps below to prepare for this assignment.

- Choose a presentation software to create your presentation.
- Consider the following guidelines as you prepare to create your presentation:

- It is suggested that you write an outline or script of what you are going to say before you begin recording in addition to having your design and supporting visuals ready. Although many software programs allow you to pause or edit, it is advisable to prepare before you start recording.
- Watch your video prior to posting to ensure that the audio volume is appropriate.

Kaltura

For this assignment, you may choose to create your presentation using Kaltura. To learn how to use Kaltura, refer to the Using Kaltura [PDF] tutorial found in the second study in this unit.

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

Directions

Prepare and record a 5–7 minute recorded presentation (with voice and supporting visuals) with content and tone appropriate for IT professionals.

Do the following in your presentation:

- Summarize the following work you completed in assignments 4 and 7 regarding the Wireless Network Security Scenario:
  - Assessing the network's ability to mitigate identified exposures.
  - Explaining how to address the identified network exposures.
- Describe a method to effectively monitor the network's controls.
- Explain two activities that would be appropriate for monitoring ongoing exposure to the network. Explain why each is appropriate.
- Summarize and explain a security policy that you believe would improve network security.

Submission Requirements

Zip and submit your presentation. You may also choose to post your presentation to a web server of your choice. If so, submit a Word document with the link to the presentation.

Course Resources
Using Kaltura [PDF]
Disability Services
DisabilityServices@Capella.edu