Preview: IAS5015 : Network Security Fundamentals and Cryptography

Syllabus

Course Overview

This course focuses on the application of fundamental concepts related to firewalls and virtual private network (VPN) solutions used to defend the confidentiality and integrity of data, as well as the best practices for managing and monitoring security solutions. Penetration and intrusion detection are also considered as are the theoretical underpinnings of cryptography and a range of information security controls and methods that use it.

The course includes step-by-step hands-on learning labs that enable you apply methods designed to secure networks.

Technology Resources

This Capella course offers labs through Jones and Bartlett Learning (JBL). These labs offer guided practice in performing tasks related to achieving course competencies and completing assessments.

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.

Disability Services

Note: 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 statistical procedures to information security data.
2. Analyze network security architecture for vulnerabilities and risk.

3. Apply security controls to mitigate risk to data confidentiality, integrity, and availability.
4. Apply cryptographic tools and techniques.
5. Communicate effectively and professionally.

Course Prerequisites

Prerequisite(s): Completion of or concurrent registration in IAS5010 or PM5331.

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.

Hardware for Kaltura

- Headset with microphone
- Broadband Internet connection

Book

Stewart, J. M. (2014). *Network security, firewalls, and VPNs* (2nd ed.). Burlington, MA: Jones & Bartlett. ISBN: 9781284031676.

Stewart, J. M. (2014). *Network security, firewalls, and VPNs* – Online labs (2nd ed.). Burlington, MA: Jones & Bartlett. ISBN: 9781284191516.

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.

- Anwar, S., Jasni, M. Z., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39–63.
- Collett, S. (2017, July 25). 5 reasons to take a fresh look at your security policy. *CSO*.
- Dhore, M. L., & Aldhaheri, R. (2017). Case study on firewall rules analysis for CWN. *International Journal of Computer Networks and Communications Security*, *5*(2), 20–27.
- Drinkwater, D. (2017, June 26). 10 steps for a successful incident response plan. *CSO*.
- Dymora, P., Mazurek, M., & Pilecki, T. (2014). Performance analysis of VPN remote access tunnels. *Annales Universitatis Mariae Curie-Sklodowska*, *14*(3), 53–64.
- Korolov, M. (2018, August 27). What are next generation firewalls? How the cloud and complexity affect them. *CSO*.
- Kumar, M., Kaur, N., Kaur, S., & Singh, R. (2016). Different security threats and its prevention in computer network. *International Journal of Advanced Research in Computer Science, 7*(6), 85–88.
- Peers, N. (2017). OpenVPN: Stay secure online. *Linux Format*, 231, 76–79.

- Rao, B. B., & Kavitha, S. (2015). Connect users to private networks securely over public networks using virtual private networks. *International Journal of Advanced Research in Computer Science*, *6*(3), 4–7.
- Sadotra, P., & Sharma, C. (2017). SQL injection impact on web server and their risk mitigation policy implementation techniques: An ultimate solution to prevent computer network from illegal intrusion. *International Journal of Advanced Research in Computer Science*, *8*(3), 678–686.
- Shao-Long, W., Wang, J., Chao, F., & Pan, Z.-P. (2016). Wireless network penetration testing and security auditing. *ITM Web of Conferences, 7*, 1–6.
- Skillsoft. (n.d.). CompTIA Network+ N10-006: Network security [Tutorial].
- Skillsoft. (n.d.). CompTIA Security+ SY0-401: Cryptographic methods and public key infrastructures [Tutorial].
- Stapleton, J. J., & Epstein, W. C. (2016). *Security without obscurity: A guide to PKI operations.* Boca Raton, FL: Auerbach.
- Ullrich, J., Cropper, J., Frühwirt, P., & Weippl, E. (2016). The role and security of firewalls in cyber-physical cloud computing. *Journal on Information Security*, 1–20.

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.

- GlobalSign. (2017). What is a man-in-the middle attack and how can you prevent it? Retrieved from https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack
- Gpg4win. (n.d.). Retrieved from https://www.gpg4win.org/
- gpgtools.org. (n.d.). GPG Suite. Retrieved from https://gpgtools.org/
- Microsoft. (2017). Microsoft security bulletin MS16-087 – Critical. Retrieved from https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-087
- Trent, R. (2016). July 2016 patch Tuesday: Gotta catch 'em all! Retrieved from https://www.itprotoday.com/threat-management/july-2016-patch-tuesday-gotta-catch-em-all

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.

- Offensive Security. (n.d.). Penetration test report [PDF]. Retrieved from https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.
- Slideshare. (n.d.). Customer pentsest report. Retrieved from https://www.slideshare.net/btpsec/btpsec-sample-penetration-test-report

Unit 1 >> Network Security and Firewall Fundamentals

Introduction

Unit 1 explores the fundamentals of network security. You learn about threats to the security of data crossing network infrastructures, and about the tools and procedures used to defend against them. It focuses particular attention on firewalls as key components of network security. You learn about what a firewall is, what it does, and how it works to permit or deny traffic based on specific criteria. You will also explore various types of firewalls and how they work to provide solutions to difficult data security challenges.

In the hands-on lab you learn to configure a pfSense Firewall on a client.

Learning Activities

u01s1 - Studies

Reading

Read the following in *Network Security, Firewalls, and VPNs*.

- Chapter 1, "Fundamentals of Network Security," pages 2–38.
- Chapter 2, "Firewall Fundamentals," pages 44–74.

Skillsoft Resources

In CompTIA Network+ N10-006: Network security [Tutorial], view:

- Security Concepts.

u01s1 - Learning Components

- Understand how firewalls operate and integrate into a network environment.
- Identify various types of firewalls.

u01s2 - Kaltura Media Preparation

An assignment in this course 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 microphone and 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 - Firewall Filtering

Firewall systems enable network security administrators to control the flow of data in and out of a network by enforcing rule sets that permit or deny traffic based on various criteria, including IP addresses, TCP and UDP port numbers, transport layer sequence numbers, and application header information.

Pick one of the following filter criteria to discuss. Choose a criterion that has not yet been exhaustively covered in the existing posts.

- IP address.
- TCP and UDP port numbers.
- Transport layer sequence numbers.
- Application header information.

Discuss how your chosen filter criterion works to permit or deny network traffic. Suggest a placement for the firewall enforcing the filtering rule within the context of an enterprise network.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u01d1 - Learning Components

- Understand how firewalls operate and integrate into a network environment.

u01v1 - Lab: Configuring a pfSense Firewall on the Client

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1: Step 28.
    - Section 2: Steps 5, 7, and 9.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources

Assignment Template

u01a1 - Enterprise Firewalls

By now you should have completed the labs in the Virtual Resource Activity for this unit and saved your screenshots to a Word document for submission with this assignment.

Overview

Information security personnel need to have an in-depth understanding of network defense concepts and techniques, including firewalls. In this assignment you apply your knowledge of how firewalls protect information assets against attacks traversing internal and external enterprise networks.

Directions

Consider your lab work and studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Create a diagram depicting how a firewall system can be effectively integrated into a typical enterprise network. **Note:** There can be multiple devices in a well-protected network. Explain the rationale for device placement(s). The network should include:
    - Switches.
    - Router(s).
    - Server(s).
    - Firewall(s).
    - DMZ.
3. Compare and contrast the primary features of pfSense and Windows Defender firewalls. Explain why one firewall may be more appropriate than the other for a large enterprise network.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Unit 2 >> Virtual Private Network (VPN) Fundamentals

Introduction

Unit 2 explores the foundations of network security with a focus on virtual private network (VPN) systems, which enable the secure transmission of enterprise data across public networks, especially the Internet. Organizational deployment of VPN technologies typically generates substantial cost savings over the use of traditional leased-line wide area network (WAN) connections. VPNs are commonly used to provide remote users with access to enterprise data resources, and to connect various network locations together using site-to-site designs. This week you will also take a closer look at threats and other issues related to network security.

In the hands-on lab you learn to configure a virtual private network server.

Learning Activities

u02s1 - Studies

Reading

Read the following in *Network Security, Firewalls, and VPNs*.

- Chapter 3, "VPN Fundamentals," pages 80–106.
- Chapter 4, "Network Security Threats and Issues," pages 113–144.

Skillsoft Resources

In CompTIA Network+ N10-006: Network Security [Tutorial], view:

- Common Threats and Vulnerabilities.

u02s1 - Learning Components

- Explain how the encryption process works in VPNs.
- Explain how encryption relates to VPNs.
- Identify principles of symmetric and asymmetric encryption.

u02d1 - VPN and Encryption

Virtual private networks (VPN) enable the transmission of encrypted data traffic across a public network in such a way as to emulate the functionality of a direct connection within a private network.

Consider your own personal or professional experience, or other exploration, of using or administering a VPN system. Discuss the following:

- Encryption standards employed.

- The potential disadvantages or limitations of VPN use.
- The role of VPN in site-to-site data transmission.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u02v1 - Lab: Configuring a Virtual Private Network Server

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - **Section 1:**
        - Part 1 – Steps 19, 28, 51, 62, and 70.
        - Part 2 – Step 9.
    - **Section 2:**
        - Part 1 – Steps 13 and 28.
        - Part 2 – Steps 3, 6, and 8.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources

Assignment Template

u02a1 - VPNs and Cryptography

By now you should have completed the labs in the Virtual Resource Activity for this unit and saved your screenshots to a Word document for submission with this assessment.

Overview

Information security personnel need to have an in-depth understanding of at network defense concepts and techniques, including VPN deployment. In this assignment you apply your knowledge of how VPNs protect information assets against attacks traversing the Internet and other public networks.

Directions

Consider your lab work and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Diagram the end-to-end cryptographic process of establishing a VPN connection. Be sure to diagram all aspects of the process, including secure symmetric key exchange, the authentication of VPN link endpoints, and the verification of both the source and integrity of transmitted data. Describe the process depicted.
3. VPN solutions may deploy both symmetric cryptography and asymmetric cryptography. Describe specific features that distinguish symmetric cryptography from asymmetric cryptography.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Unit 3 >> Network Security Implementation and Management

Introduction

Unit 3 begins the technical overview of network security, firewalls, and virtual private networks (VPNs), with a particular focus on designing, installing, deploying, and configuring network security. You learn about the importance of defense in depth, the management of secure communications systems, and system hardening. Issues related to network security management are covered with an emphasis on understanding the dynamic nature of network security, and the need for constant vigilance in the face of an ever changing threat landscape.

In the hands-on lab you investigate and respond to security incidents.

Learning Activities

u03s1 - Studies

Reading

Read the following in *Network Security, Firewalls, and VPNs*:

- Chapter 5, "Network Security Implementation," pages 151–176.
- Chapter 6, "Network Security Management," pages 182–208.

Read the following in the Capella Library:

- Drinkwater, D. (2017, June 26). 10 steps for a successful incident response plan. *CSO*.
    - This resource identifies steps to create a successful incident response plan.

Read the following on the Internet:

- Trent, R. (2016). July 2016 patch Tuesday: Gotta catch 'em all! Retrieved from https://www.itprotoday.com/threat-management/july-2016-patch-tuesday-gotta-catch-em-all
    - This resource identifies the severity level of various Microsoft updates.
- Microsoft. (2017). Microsoft security bulletin MS16-087 – Critical. Retrieved from https://docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-087
    - This resource addresses a Microsoft Windows print spooler remote code execution vulnerability.

Skillsoft Resources

In CompTIA Network+ N10-006: Network Security [Tutorial], view:

- Network Hardening.

u03s1 - Learning Components

- Outline steps to address an exploitation such as those on a Windows print spooler.
- Understand basic incident response protocols.

- Review examples of incident response plans.
- Review Microsoft Security Bulletin MS16-087.

u03s2 - 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.

u03d1 - Security Breaches

Research a specific case, or speak from your own personal or professional experience, of a significant physical security breach of a computing environment.

Discuss the following:

- Attack vectors and techniques use to carry out the attack.
- Probable motivation of the attacker.
- How the incident was detected.
- Steps taken to mitigate the effects of the attack.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u03v1 - Investigating and Responding to Security Incidents

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 1 – Steps 8, 17, 22, and 28.
        - Part 2 – Steps 6 and 11.
    - Section 2:
        - Part 1 – Steps 4, 6, 9, 17, 20, 23, and 25.
        - Part 2 – Steps 3, 5, and 15.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources

Assignment Template

u03a1 - Intrusion Assessment and Response

By now you should have finished sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

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 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.

Preparation

Read Microsoft Security Bulletin MS16-087, found in the Resources.

Scenario

Imagine that you are a network security administrator and you receive a critical alert from an intrusion detection system (IDS) regarding the ingress transmission of code execution targeting the exploitation of Windows print spooler components vulnerabilities identified in Microsoft Security Bulletin MS16-087.

Directions

Consider your lab work and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots. Be specific.
2. 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:
    - Introduce the nature of the intrusion and the systems likely affected.
    - Outline the steps necessary to effectively assess this security incident.
    - Create and explain a security incident response plan designed to mitigate the exploitation. Make sure to:
        - Reference relevant security bulletins that exist (perform an Internet search).
        - Explain key components of your recommended technical solution.

Submission Instructions

Submit your presentation and the Word document with your screenshots.

Course Resources
Microsoft Security Bulletin MS16-087 – Critical
DisabilityServices@Capella.edu

Unit 4 >> Fundamentals of Firewall Deployment

Introduction

Unit 4 continues the technical overview of network security, firewalls, and virtual private networks (VPNs), with a particular focus on firewall technologies. A firewall is typically an important feature of an enterprise network infrastructure, and may range from quite simple to extremely complex in design. You learn about how firewalls interact with intrusion detection and other monitoring systems. A focus on firewall design principles, including least privilege, simplicity, defense in depth, and universal participation informs your understanding of firewall deployment considerations.

In the hands-on lab you configure a firewall server.

Learning Activities

u04s1 - Studies

Reading

Read the following in *Network Security, Firewalls, and VPNs*:

- Chapter 7, "Firewall Basics," pages 213–243.
- Chapter 8, "Firewall Deployment Considerations," pages 248–269.

Read the following in the Capella Library:

- Kumar, M., Kaur, N., Kaur, S., & Singh, R. (2016). Different security threats and its prevention in computer network. *International Journal of Advanced Research in Computer Science, 7*(6), 85–88.

    - This resource identifies network security threats and details preventative measure to protect a computer network.

- Dhore, M. L., & Aldhaheri, R. (2017). Case study on firewall rules analysis for CWN. *International Journal of Computer Networks and Communications Security*, *5*(2), 20–27.
    - This resource explains an approach for analyzing rules implemented on a firewall to find hidden anomalies.

Skillsoft Resources

In CompTIA Network+ N10-006: Network Security [Tutorial], view:

- Network Access Control Models.

u04s1 - Learning Components

- Understand the security issues related to spoofing, and broadcast and outbound traffic.
- Review examples of firewall rules.
- Understand the principles behind spoofing, and broadcast and outbound traffic.

u04d1 - Firewall Breaches

Research a specific case, or speak from your own personal or professional experience, of a significant firewall breach of an enterprise network environment, and discuss the attack vectors and techniques used to carry out the attack, the probable motivation of the attacker, how the incident was detected, and the steps taken to mitigate the effects of the attack.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u04v1 - Configuring a pfSense Firewall on the Server

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 1 – Steps 10 and 15.
        - Part 2 – Step 7.
    - Section 2:
        - Part 1 – Steps 7 and 11.
        - Part 2 – Steps 3 and 9.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources
Assignment Template

u04a1 - Firewall Rules

By now you should have finished Sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

Scenario

Imagine that you are a security consultant working to test a firewall security solution in a small enterprise network. You discover that the enterprise's firewall has permit and deny rules applied only to ingress traffic. The

enterprise's security policy explicitly requires that the firewall block egress IP spoofing, block broadcast traffic, and block all outbound traffic from internal servers.

Directions

Consider your lab work and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Explain the reasons for having the firewall rules stated in the scenario above.
3. Construct a firewall rule to block each of the following from internal servers on the 209.222.18.0 network (**Note:** use this structure: *[Protocol] [Source Address] [Source Port] [Target Address] [Target Port] [Action]:*
    - Egress IP spoofing.
    - Broadcast traffic.
    - Outbound traffic.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Unit 5 >> Managing Firewall Security

Introduction

Unit 5 continues the technical overview of network security, firewalls, and virtual private networks (VPNs), with a particular focus on firewall management and using common firewall systems. You will learn about the essential security goals of enterprise environments and understand how firewalls serve to realize those goals. Firewall selection will be considered, as will basic firewall configuration considerations. Issues related to network security management, particularly firewall testing, monitoring, and troubleshooting will be central to this week's study, as will ideas about the actual deployment of firewalls in an enterprise networking environment.

In the hands-on lab you perform penetration testing on a firewall.

Learning Activities

u05s1 - Studies

techniques use to carry out the attack, the probable motivation of the attacker, how the incident was detected, and the steps taken to mitigate the effects of the attack. Also, discuss the ways in which social engineering may be an important skill for a professional pen tester.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u05d1 - Learning Components

- Explain penetration testing methodology.

u05v1 - Penetration Testing a pfSense Firewall

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 2 – Steps 11, 13, and 27.
    - Section 2:
        - Part 1 – Step 4.
        - Part 2 – Steps 6, 8, 13, and 21.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Readings

Read the following in *Network Security, Firewalls, and VPNs*:

- Chapter 9, "Firewall Management and Security," pages 275–296.
- Chapter 10, "Using Common Firewalls," pages 301–318.

Read the following from the Capella Library:

- Shao-Long, W., Wang, J., Chao, F., & Pan, Z.-P. (2016). Wireless network penetration testing and security auditing. *ITM Web of Conferences, 7*, 1–6.
    - This resource discusses ways that penetration testing and auditing help to mitigate the risk and threatens to wireless local area networks.

Skillsoft Resources

In CompTIA Network+ N10-006: Network Security [Tutorial], view:

- Firewalls.

Optional Reading

- Offensive Security. (n.d.). Penetration test report [PDF]. Retrieved from https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.
    - A sample penetration test report.
- Slideshare. (n.d.). Customer pentsest report. Retrieved from https://www.slideshare.net/btpsec/btpsec-sample-penetration-test-report

u05s1 - Learning Components

- Identify penetration testing tools.
- Explain penetration testing methodology.
- Review examples of firewall penetration tests.
- Describe penetration testing hardware and software tools.
- Understand components of penetration test reports.

u05d1 - Socially Engineered Security Breaches

Attempts at social engineering are commonly included in a comprehensive penetration test. Research a specific case, or speak from your own personal or professional experience, of a significant security breach of an enterprise network environment that was achieved using social engineering, and discuss the attack vectors and

Course Resources

Assignment Template

u05a1 - Penetration Tools and Testing

By now you should have finished Sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

Overview

Effective penetration testing consists of fine main steps: reconnaissance, scanning, vulnerability analysis (enumeration), exploitation (the actual attack), and post-attack activities, including remediation of the vulnerabilities. Before attacking a system, the pen tester first typically utilizes automated tools to scan for and identify the various vulnerabilities that can be exploited.

Directions

Consider your lab work and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Compare and contrast three security tools that enable a penetration tester to configure unauthorized tunnels through an enterprise firewall. Make sure to identify specific features that distinguish them from one another.
3. Imagine that you are a security consultant working to identify vulnerabilities of a firewall security solution in a small enterprise network. Write a firewall penetration testing plan that (make and state assumptions as required to support your choices):
   a. Explains the specific tests to be run.
   b. Explains the test methodology.
   c. Lists 3 deliverables that would be a part of a post penetration test technical report. For example, one might include the success rate of deployed social-engineering methods.
   d. Describes the hardware and software tools to be deployed and why they are appropriate.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Unit 6 >> Managing VPN Technologies

Introduction

This unit continues the technical overview of network security, especially regarding the management of VPN technologies. Proactive management of VPNs is often a critical function of an enterprise's information security team duties because of the way in which VPNs enable internal enterprise information assets to be accessed via public networks—particularly the Internet. You learn how to determine when a VPN may be optimal for a particular context, and explore the options for selection and installation of VPN components.

In the hands-on lab you configure a VPN client to support secure file transfer.

Learning Activities

u06s1 - Studies

Reading

Read the following in *Network Security, Firewalls, and VPNs*.

- Chapter 11, "VPN Management," pages 323–343.
- Chapter 12, "VPN Technologies," pages 352–370.

Read the following in the Capella Library:

- Peers, N. (2017). OpenVPN: Stay secure online. *Linux Format*, 231, 76–79.
  - This resource discusses features of an OpenVPN solution.
- Dymora, P., Mazurek, M., & Pilecki, T. (2014). Performance analysis of VPN remote access tunnels. *Annales Universitatis Mariae Curie-Sklodowska*, *14*(3), 53–64.
  - This article focuses on various VPN protocols and technologies.
- Rao, B. B., & Kavitha, S. (2015). Connect users to private networks securely over public networks using virtual private networks. *International Journal of Advanced Research in Computer Science*, *6*(3), 4–7.
  - This resource addresses various VPN designs that can be deployed to provide secure connectivity over a public network.

u06s1 - Learning Components

- Explain OpenVPN, PPTP, L2TP protocols.

- Explain remote access and site-to-site VPN tunnels.
- How to maximize performance in a high-latency network.

u06d1 - VPN Breaches

Research a specific case, or speak from your own personal or professional experience, of a significant security breach of a VPN system.

Discuss the following:

- The attack vectors and techniques use to carry out the attack.
- The probable motivation of the attacker.
- How the incident was detected, and the steps taken to mitigate its effects.
- How using VPN management best practices might have prevented the breach.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u06v1 - Configuring a VPN Client for Secure File Transfer

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:

        - Part 1 – Steps 27 and 66.
        - Part 2 – Steps 12, 29, 45, 50, and 52.
    - Section 2:
        - Part 1 – Steps 19 and 22.
        - Part 2 – Steps 5, 20, and 22.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources
Assignment Template

u06a1 - Configuring a VPN Client for Secure File Transfer

By now you should have finished Sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

Overview

Virtual private networks (VPNs) enable the secure transmission of data across a network that may not have security built in, such as the Internet. In this assignment, you consider three major types of VPN connections that can be implemented to secure data; a tunnel VPN, a transport VPN, and a pass-through VPN.

Directions

Consider your lab work and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Compare and contrast four encryption protocols; OpenVPN, PPTP, L2TP, and one more of your choice.
3. Analyze the above VPN protocols and explain which are appropriate or effective for:
    - Constructing remote access VPN tunnels.
    - Constructing site-to-site VPN tunnels.

- Providing maximum performance in a high-latency network.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Course Resources
Configuring a VPN Client for Secure File Transfer

Unit 7 >> Firewall Implementation and Real-World VPNs

Introduction

This unit examines the implementation of firewall and VPN systems. You consider how to examine an enterprise network in order to determine security requirements, and learn about issues related to the successful configuration, testing, and troubleshooting of firewall and VPN deployments. A focus on best practices makes clear some of the technical aspects of creating reliable protection for the confidentiality and integrity of data exchanged via the network and Internet. Consideration is also be given to intranet and extranet solutions.

In the hands-on lab you learn to defend a VPN from attack.

Learning Activities

u07s1 - Studies

Reading

Read the following in *Network Security, Firewalls, and VPNs*.

- Chapter 13, "Firewall Implementation," pages 375–390.
- Chapter 14, "Real-World VPNs," pages 395–415.

Read the following in the Capella Library:

- Collett, S. (2017, July 25). 5 reasons to take a fresh look at your security policy. *CSO*.
  - This resource identifies points regarding updating security policies.

Read the following on the Internet:

- GlobalSign. (2017). What is a man-in-the middle attack and how can you prevent it? Retrieved from https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack
    - This article describes the features of common man-in-the-middle (MITM) attacks.

u07s1 - Learning Components

- Recognize common network vulnerabilities.
- Understand MITM attacks.
- Explain elements of a security policy.

u07d1 - Small Business Risk

A popular architecture for organizations when the Tootsie Pop strategy was developed and widely implemented was static data that largely remained behind the firewall. The line of demarcation was very clear. The ability to protect the firewall by opening very narrow point-to-point connections and opening a small number of commonly used ports and services made the firewall a relatively powerful tool that unfortunately was soon perceived as the be-all and end-all of security. Some network administrators who employed firewalls became a little too complacent. The idea that Port 80 would be used for the degree of malware and maliciousness that is now possible was not even on the horizon. Today, the seemingly ubiquitous access to enterprise data by personal devices, enabled by bring your own device (BYOD) policies, coupled with often frequent use of public Internet hot spots, presents new challenges to information security professionals.

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

Discuss the following:

- Make a case for why the Tootsie Pop strategy is still important and useful.
- Make a case for why the Tootsie Pop strategy is outdated and no longer a viable way to think about network security.
- Suggest how an enterprise security policy could ensure deployment of the next emerging firewall strategy that might be a good replacement for the Tootsie Pop strategy.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u07v1 - Attacking a Virtual Private Network

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 1 –Steps 10 and 16.
        - Part 2 – Step 4.
    - Section 2:
        - Part 1 – Steps 24 and 38.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources
Assignment Template

u07a1 - Attacking a Virtual Private Network

By now you should have finished sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

Scenario

Creative Breweries has decided to branch out from their craft beer line to include a new line of distilled beverages. They hire a new employee who needs to work offsite from her home office, as well as have the ability to remotely control her home desktop from her laptop while traveling.

The company has recently experience a significant data breach following a man-in-the-middle (MITM) attack on an employee connecting with a laptop to enterprise data resources from a public Internet hot spot located at a popular coffee house chain location. They are keen to address the vulnerability.

Directions

Consider the scenario, your lab work, and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Analyze the scenario and briefly explain what an MITM attack is, and explain the possible security threats it poses.
3. Write a VPN policy in response to the security incident that is designed to provide assure reasonable confidentiality for highly sensitive data and meets the needs of the new employee.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Unit 8 >> The Future of Firewalls and VPNs

Introduction

In Unit 8, we consider the future of firewall and VPN solutions in the face of an ever-evolving security landscape that will undoubtedly present new risks and vulnerabilities. Cryptography is also introduced including a study of asymmetric and symmetric encryption algorithms, digital signatures, one-way hashing, key life cycle management controls, and a variety of security protocols. Also explored are concepts related to a public key infrastructure (PKI), which is a subset of the cryptography field, which is founded upon mathematics based on number theory.

In the hands-on lab you deploy a protocol analyzer to monitor network traffic.

Learning Activities

u08s1 - Studies

Reading

Read the following in *Network Security, Firewalls, and VPNs*.

- Chapter 15, "Perspectives, Resources, and the Future," pages 419–437.

Read the following in the Capella Library:

- Korolov, M. (2018, August 27). What are next generation firewalls? How the cloud and complexity affect them. *CSO*.
    - This resource evaluates the functionality of nextgen firewalls with cloud, mobile, and endpoint protection.
- Anwar, S., Jasni, M. Z., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39–63.
    - This article discusses the relationship of firewalls to intrusion detection systems.
- Ullrich, J., Cropper, J., Frühwirt, P., & Weippl, E. (2016). The role and security of firewalls in cyber-physical cloud computing. *Journal on Information Security*, 1–20.
    - This article discusses the role of firewalls in protecting cloud computing systems.

Skillsoft Resources

In CompTIA Network+ N10-006: Network Security [Tutorial], view:

- Physical Security.

u08s1 - Learning Components

- Ability to use and interpret a traffic analysis tool data.
- Ability to use data from a spreadsheet to graphically depict data.

u08d1 - Network Traffic Security Analysis

A protocol analyzer (also known as a packet analyzer) is a tool used to intercept and log traffic transiting a digital network. The careful analysis of captured traffic may be critical to supporting network operations and information security functions. Discuss the following:

- Protocol analyzers can be either software- or hardware-based. What are some of the limitations of software packet analyzers?
- What security precautions do you recommend for network personnel who perform packet capture activities in an enterprise environment?

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u08v1 - Using Wireshark and Netwitness to Analyze Wireless Traffic

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:
        - Part 1 – Steps 18, 37.
        - Part 2 – Step 13.
    - Section 2:
        - Part 1 – Steps 7, 15, 18, 20, 22, 24, 26.
        - Part 2 – Steps 6, 9.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

- E-mail: support@jblearning.com

- Phone: 1-800-832-0034, option 5.

Course Resources

Assignment Template

u08a1 - Using Wireshark and Netwitness Investigator to Analyze Wireless Traffic

By now you should have finished Sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

Overview

Security administrators routinely deploy tools to monitor and analyze ingress and egress traffic transiting enterprise networks. Wireshark is one of the most widely used packet capture and analysis tools. It enables the capture of network packet traffic and the capability to save frame details in multiple formats that make them usable by the more sophisticated, more expensive software tools.

Directions

Consider your lab work and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. In the PacketCapture.pcapng file you reviewed in Section 1 of the lab, there is a lot of traffic for the TLSv1 protocol. Explain the primary function of the bulk of the traffic.
3. In the lab, apply a filter to the HotspotCapture.pcapng file that will display only the packets related to Address Resolution Protocol (ARP). Identify the device used and take a screenshot showing the results of the filtered data and include it in your assignment submission.
4. Apply the same filter to three other protocols and create a spreadsheet and associated histogram that depicts the volume of traffic for each protocol.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Unit 9 >> Fundamentals of Cryptography

Introduction

This unit focuses on fundamental ways in which cryptography may be used in an enterprise computing environment to support the CIA triad of confidentiality, integrity, and availability. You examine the role of public key infrastructure (PKI) in enabling a host of various security controls and explore concepts related to security standards, protocols, and infrastructure architectural components. Consideration is given to some of the mathematical research that enables the development of the hardware, firmware, and software vital to the operations of modern security solutions.

In the hands-on lab you deploy encryption to enable the confidentiality and integrity of enterprise data assets.

Learning Activities

u09s1 - Studies

Reading

Read the following in the Capella Library:

- Stapleton, J. J., & Epstein, W. C. (2016). *Security without obscurity: A guide to PKI operations.* Boca Raton, FL: Auerbach.
  - Chapter 1, "Introduction," pages 1–18.
  - Chapter 4, "PKI Management and Security," pages 19–60.
  - Chapter 5, "PKI Roles and Responsibilities," pages 61–100.

Skillsoft Resources

In CompTIA Security+ SY0-401: Cryptographic Methods and Public Key Infrastructures [Tutorial], view:

- Cryptography.
- Symmetric Encryption.
- Asymmetric Encryption.

u09s1 - Learning Components

- Understand encryption fundamentals.
- Explain how to encrypt using a public key.

u09d1 - Enterprise Encryption Policies

Consider the encryption efforts of one of your current or past employers, or research a typical enterprise network and discuss the following:

- Where is encryption deployed in the enterprise, and what critical data or business process is it protecting?
- How does the organization handle management of cryptographic keys?
- Explain the policies, tools, and/or protocols used for key generation, key exchange, key storage, key use, key destruction, and replacement of lost keys.

You are encouraged to interview appropriate personnel at the organization as part of your research.

Response Guidelines

Read the posts of your peers and respond to two (minimum) and expand on the concepts covered in their initial post. 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

u09d1 - Learning Components

- Understand encryption fundamentals.

u09v1 - Using Encryption to Enhance Confidentiality and Integrity

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
    - Section 1:

        - Part 1 – Steps 11, and 17.
        - Part 4 – Step 22.
    - Section 2:
        - Part 1 – Steps 5 and 9.
        - Part 2 – Step 4.
        - Part 3 – Step 5.

Jones & Bartlett Technical Support

If you have technical issues pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources
Assignment Template

u09a1 - Using Encryption to Enhance Confidentiality and Integrity

By now you should have finished sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

Overview

Confidentiality, integrity, and availability comprise the famous CIA triad of information security. Encryption is an increasingly important way to assure data confidentiality and integrity. In this week's assignment and lab you apply encryption technology to achieve both using encryption keys.

Preparation

Do one of the following. Links are in the Resources:

- Install Gpg4win on your own local Windows machine.
- Install GPG Suite on your own local Apple machine.

Directions

Consider your lab work and other studies to address each of the following in the Word document that contains your lab screenshots. Clearly label each section.

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Determine whether it is possible to encrypt the secret-message.txt file found in the lab by using only the TargetWindows02 (receiver's) public key. Explain the ramifications of doing this as opposed to another method.
3. Create your own personal key pair using the appropriate application found in the preparation area. Use it to encrypt your Unit 8 assignment Word document, and submit it.

Submission Instructions

Submit:

- Parts one and two in a Word document with well-labeled responses.
- The encrypted Unit 8 assignment.

Course Resources
Gpg4win
GPG Suite

Unit 10 >> PKI Encryption Management and Security

Introduction

In this final unit of the course we will turn our attention to thinking about PKI security management and the roles and responsibilities of a wide variety of stakeholders, including PKI, administrators, technicians, custodians, security officers, subscribers, relying parties, security managers, and auditors. You also explore the primary functions of certificate authorities, root CAs, registration authorities, policy authorities, and online certificate status protocol (OCSP) operations.

In the hands-on lab you deploy digital signatures to authenticate the source of data communications.

Learning Activities

u10s1 - Studies

Reading

Read the following in the Capella Library:

- Stapleton, J. J., & Epstein, W. C. (2016). *Security without obscurity: A guide to PKI operations*. Boca Raton, FL: Auerbach.
  - Chapter 4, "PKI Management and Security," pages 101–161.
  - Chapter 5, "PKI Roles and Responsibilities," pages 162–182.
- Sadotra, P., & Sharma, C. (2017). SQL injection impact on web server and their risk mitigation policy implementation techniques: An ultimate solution to prevent computer network from illegal intrusion. *International Journal of Advanced Research in Computer Science*, *8*(3), 678–686.

Skillsoft Resources

In CompTIA Security+ SY0-401: Cryptographic Methods and Public Key Infrastructures [Tutorial], view:

- Public Key Infrastructures and Certificate Authorities.
- Cryptographic Security.

u10s1 - Learning Components

- Understand how specific network security issues affect a network.
- Ability to use data from a spreadsheet to graphically depict data.
- Understand traffic flow measurement data.
- Understand components of a data set generated by a network monitoring tool.

u10v1 - Authenticating Security Communications with Digital Signatures

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Sections 1 and 2 of the lab.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots during the lab:
   - Section 1:
     - Part 1 – Step 18.

        - Part 2 – Step 9.
        - Part 3 – Step 8.
    - Section 2:
        - Part 3 – Steps 6, 12, 15, and 17.

Jones & Bartlett Technical Support

If you have technical issue pertaining to accessing JBL virtual labs, contact JBL Technical Support:

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

Course Resources

Assignment Template

u10a1 - Analyzing Network Monitoring Tool Data

By now you should have finished Sections 1 and 2 of the unit lab and saved your screenshots to a Word document.

Overview

Big data and data analytics are hot topics in the media these days. Much of the application of these mathematical concepts is industry specific, and the information security industry is no exception. Math plays an important role in an array of methods and technologies. One of the earlier applications of math in computer technology involved calculating subnets and creating encryption algorithms. In this assignment, you will analyze a data set collected by a network monitoring tool to identify security issues, apply statistical procedures to the data, and write a meaningful interpretation of the data.

Preparation

Review the Data Set document found in the Resources. It represents security events data generated by a network monitoring tool. Use it to complete the assignment.

Directions

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

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
2. Examine the Data Set using MS Excel or other appropriate application and answer the following:
    - Which of the security issues indicated in the data do you believe is the most serious security problem? Explain your rationale.
3. Create a histogram that displays the number of occurrences associated with five of the security issues shown in the data. Include the spreadsheet data used to generate your histogram.

Submission Instructions

Submit your assignment in a Word document with well-labeled responses.

Course Resources
Data Set

u10d1 - Course Reflection

Share the aspects of this course that you found most useful and describe how those skills will enhance your professional goals. Responses to peers are not required.

Course Resources
Graduate Discussion Participation Scoring Guide