Syllabus

Course Overview

This course focuses on the application of fundamental concepts related to operating system security solutions deployed as part of a defense in depth strategy to protect the confidentiality, integrity, and availability of data. Best practices for managing and monitoring proactive security solutions for both proprietary and open source operating systems are considered, as are operating systems security issues related to mobile computing and cloud computing. The course includes step-by-step hands-on learning labs that enable you to apply methods designed to secure Linux and Windows operating systems.

Technology Resources

This Capella course offers labs through Jones & Bartlett Learning. 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. Analyze information security vulnerabilities, threats, and risks related to computer operating systems.
2. Describe operating system defenses that are part of a layered defense-in-depth strategy.
3. Apply tools to harden computer operating systems and protect associated software applications.

4 Communicate effectively and professionally.

Course Prerequisites

Prerequisite(s): Completion of or concurrent registration in IAS5020.

Syllabus >> Course Materials

Required

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

Integrated Materials

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

Book

Capella University (Ed.). (2019). *IAS5025: Operating system defense* [Custom online lab bundle]. Burlington, MA: Jones & Bartlett.

Jang, M. and Messier, R. (2017). Security Strategies in Linux Platforms and Applications (2nd ed.). Burlington, MA: Jones & Bartlett. ISBN: 9781284090659

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

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.

- Doherty, J. *Wireless and mobile device security* (1st ed.). Burlington, MA: Jones & Bartlett Learning.
- Hall, C. (2018). Microsoft brings Linux driven IoT security to Azure. *Windows IT Pro* (Online).
- Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97–114.
- Hellard, B. (2018). Windows vs Linux: What's the best operating system? *IT Pro.*
- Hendry, B. (2018). Team Foundation Server 2017: Internet Explorer Enhanced Security Configuration [Video]. Skillsoft, Ireland.
- Jasek, R. (2015). Security deficiencies in the architecture and overview of android and iOS mobile operating systems. Paper presented at the International Conference on Cyber Warfare and Security, 153–X.
- Joh, H. & Malaiya, Y. K. (2017). Periodicity in software vulnerability discovery, patching and exploitation. *International Journal of Information Security, 16*(6), 673–690.
- Kundu, A., & Bano, P. (2015). SELinux & Linux repository: Introduction. *International Journal of Advanced Research in Computer Science.*
- Kuļešovs, I., Borzovs, J., Susters, A., Arnicane, V., Arnicans, G., Keiduns, K., & Skutelis, J. (2018). An approach for iOS applications' testing. *Baltic Journal of Modern Computing, 6*(1), 56–91.
- Lachance, D. (2014). CompTIA Cloud+: Changing the Attack Surface [Video]. Skillsoft, Ireland.
- Lachance, D. (2015). Certified Cloud Security Professional (CCSP): Operating System Security [Video]. Skillsoft, Ireland.
- Lachance, D. (2015). Cloud Computing Technology Fundamentals: Cloud Network Infrastructure Security [Video]. Skillsoft, Ireland.
- Lachance, D. (2015). CompTIA Cloud+: Host Hardening [Video]. Skillsoft, Ireland.
- Lachance, D. (2015). CompTIA Mobility+: Mobile Device Management [Video]. Skillsoft, Ireland.
- Lachance, D. (2015). RHEL 7: Adding or Deleting an iptable Rule [Video]. Skillsoft, Ireland.
- Lachance, D. (2015). RHEL 7: Describing iptable Rules and Configuration [Video]. Skillsoft, Ireland.

- Lachance, D. (2015). RHEL 7: Saving and Restoring iptable Rulesets [Video]. Skillsoft, Ireland.
- Lachance, D. (2015). Security Trends: Mobile Devices and Malware [Video]. Skillsoft, Ireland.
- Lachance, D. (2016). Windows Server 2016 - Identity: Password policy settings [Video]. Skillsoft, Ireland.
- Lachance, D. (2017). UNIX Essentials: Enabling SSH Public Key Authentication [Video]. Skillsoft, Ireland.
- Morimoto, R. (2017). Top 5 Windows Server 2016 features that enterprises are deploying. *Network World* (Online).
- Pathak, N., & Sharma, N. (2018). Object oriented secure modeling using SELinux trusted operating system. *International Journal of Advanced Networking and Applications.*
- Rashid, F. Y. (2016). Lockdown! Harden Windows 10 for maximum security. *InfoWorld.com*.
- Rountree, D. & Castrillo, I. (2014). *The basics of cloud computing: Understanding the fundamentals of cloud computing in theory and practice.* Syngress Publishing.
- 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.
- Samani, R., Honan, B., & Reavis, J. (2015). *CSA guide to cloud computing: Implementing cloud privacy and security.* Syngress Publishing.
- Sampson, A. (2017). CompTIA Network+ N10-007: Password Policy [Video]. Skillsoft, Ireland.
- Savill, J. (2014). Azure active directory vs. on-premises active directory. *Windows IT Pro* (Online).
- Solomon, M. G. (2014). *Security strategies in Windows platforms and applications* (2nd ed.). Burlington, MA: Jones & Bartlett.
- Strom, D. (2016). 10 cutting-edge tools that take endpoint security to a new level. *Network World* (Online).
- Tozzi, C. (2018). Windows vs. Linux vs. mac vs. whatever: Does it matter? *Windows IT Pro (Online).*
- Vacca, J. R. (2017). *Security in the private cloud.* CRC Press.
- Venafi, Inc. researchers submit patent application, "System for managing cryptographic keys and trust relationships in a secure shell (ssh) environment," for approval. (2014, Nov 13). *Computer Weekly News.*
- Weinberger, M. (2015). The world of containers doesn't end with Docker. Computerworld Digital Magazine.
- Welton, T. (n.d.). Microsoft Security Fundamentals: Operating System Security. Skillsoft, Ireland.
- Welton. T. (2015). Microsoft Security Fundamentals: Microsoft Baseline Security Analyzer (MBSA) [Video]. Skillsoft, Ireland.
- Yates, J. (2015). Windows 10: Countermeasures. Skillsoft, Ireland.
- Yuksel, A. S., Zaim, A. H., & Aydin, M. A. (2014). A comprehensive analysis of Android security and proposed solutions. *International Journal of Computer Network and Information Security, 6*(12), 9–20.

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.

- Anicas, M. (2015). Iptables essentials: Common firewall rules and commands. Retrieved from https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands
- Firewalld.org. (2018). HowTo. Retrieved from https://firewalld.org/documentation/howto/
- Kazim, M., Masood, R., Shibli, A. (2013). Security aspects of virtualization in cloud computing. Retrieved from https://www.researchgate.net/publication/273950406_Security_Aspects_of_Virtualization_in_Cloud_Computing
- Keary, T. (2018). 6 best alternatives to Microsoft Baseline Security Analyzer. Retrieved from https://www.comparitech.com/net-admin/alternatives-to-microsoft-baseline-security-analyzer/

- Ohlinger, M. (2014). How to create a Windows Firewall Inbound Rule. Retrieved from https://blogs.msdn.microsoft.com/mandi/2014/11/03/how-to-create-a-windows-firewall-inbound-rule/
- Sciberras, N. (2014). Configuring your Web server to not disclose its identity. Retrieved from https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/

Suggested

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

Optional

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

External Resource

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

- Microsoft. (2017). Windows Server 2016 security: Better protection begins at the OS. Retrieved from http://download.microsoft.com/download/6/7/3/673E651E-C5B3-4C93-A69A-94042EB6DE22/Windows_Server_2016_Security_Better_protection_begins_at_the_OS_Whitepaper_EN_US.pdf

Unit 1 >> Introduction to Operating Systems Security

Introduction

This week you will:

- Be introduced to the fundamentals of OS security.
- Discuss Linux Boot Loaders and security levels of various OSs.

Unit 1 introduces the fundamentals of operating systems security. You explore the importance of protecting operating systems from attack with particular attention on Microsoft Windows, as well as common Linux distributions, the security of which is a key element in realizing an effective defense-in-depth strategy in an enterprise information technology environment. Also considered are the Windows operating system architecture, the Linux kernel, and some of the security controls native to various versions or distributions of these popular operating systems.

Learning Activities

u01s1 - Studies

Readings

Read the following in your course texts to become familiar with OS security basics:

- *Security Strategies in Linux Platforms and Applications* text:
  - Chapter 2, "Basic Components of Linux Security," pages 18–43.

Read the following in the Capella Library:

- Read the following in your *Security Strategies in Windows Platforms and Applications* text:
  - Chapter 2: "Security in the Microsoft Windows Operating System," pages 19–37.
- Hellard, B. (2018). Windows vs Linux: What's the best operating system? *IT Pro.*
  - This article explores the pros and cons of Windows v. Linux operating systems.
- Tozzi, C. (2018). Windows vs. Linux vs. mac vs. whatever: Does it matter? *Windows IT Pro* (Online).
  - This article addresses the primary features of Windows, Linux, and Mac OS operating systems.

Skillsoft Video

View the following video:

- Welton, T. (n.d.). Microsoft Security Fundamentals: Operating System Security [Video]. Skillsoft, Ireland.

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 - Which OS is the Most Secure

Threats confronting enterprise information systems and networks continue to rapidly evolve, with new attacks being created every day. The prevalence of computer attacks by organized crime, as well as by well-funded government-sponsored hackers, means that network and system security administrators need to be more sophisticated than ever in building robust security controls, particularly those that defend the confidentiality, integrity, and availability of data residing on enterprise computers. Given this situation, it is of paramount importance that information technologists deploy secure operating systems.

Discuss which operating system is the most secure for general deployment in an enterprise computing environment. You must take a specific position, identify your own biases based on your professional or personal experience, and defend your argument using evidence from your reading and 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

u01d2 - Linux Boot Loaders

Protecting the confidentiality, integrity, and availability of enterprise data starts from the moment a computing device is turned on. Based on your professional or personal experience, or your reading and research, describe the primary features of one of the following Linux boot loaders:

- GNU GRUB.
- LILO.
- BURG.
- Syslinux.

Discuss the following:

- The role of the Linux boot loader in the initialization process.
- How the boot loader can be configured to secure a system through the boot process.
- Some specific Linux security issues beyond the boot process. For example those associated with runlevels, services, and the graphical user interface (GUI).

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

Unit 2 >> Managing and Maintaining Microsoft Windows Security

Introduction

This week you will:

- Create a presentation on implementing Active Directory for access control.
- Implement access controls with Windows Active Directory in a virtual lab.

Unit 2 begins our exploration of specific steps available to secure Windows operating systems using built-in security features. Concepts related to the design and implementation of effective access controls are covered in the context of the principle of least privilege. Studies address security controls designed to prevent malicious software (malware) programs from violated the confidentiality, integrity, and availability of enterprise data.

Learning Activities

u02s1 - Studies

Readings

Read the following in the Capella Library:

- Read the following in your *Security Strategies in Windows Platforms and Applications* text:
  - Chapter 3, "Access Controls in Microsoft Windows," pages 40–67.
- Savill, J. (2014). Azure active directory vs. on-premises active directory. Windows IT Pro (Online).
  - This article identifies key differences between a traditional on-premises deployment of Active Directory and the trend towards cloud-based deployments of Active Directory.

Skillsoft Resources

View the following video:

- Lachance, D. (2015). Certified Cloud Security Professional (CCSP): Operating System Security [Video]. Skillsoft, Ireland.
    - After watching this video, you will be able to define operating system hardening techniques with reference to OS: Windows, Linux, VMware, etc.

u02s1 - Learning Components

- Understand fundamentals of Windows workgroups.
- Understand Windows domain fundamentals.
- Understand how to implement Active Directory.
- Understand best practices for managing Windows users.
- Describe Windows access permissions, models and controls.

u02d1 - OS Systems-based Access Control

Consider the operating system-based access control mechanisms in use at one of your current or past employers, or research a typical enterprise information technology infrastructure, and discuss the following:

- The principle of least privilege - what it is, why it is used, and ways it is implemented.
- The differences between identification, authentication, and authorization.
- A modern operating system-based access control method deployed in the enterprise.

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

u02d1 - Learning Components

- Differentiate between identification, authentication, and authorization.
- Explain the principle of ‘least privilege.'

u02s2 - 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.

u02v1 - Jones & Bartlett Lab: Implementing Access Controls with Windows Active Directory

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.

Overview

This week's hands-on lab provides you with an opportunity to configure Active Directory (AD) to enhance the confidentiality, integrity, and availability of enterprise data. You will learn how to organize users and computers into security groups to maximize access control to enterprise information resources. You will configure AD on a domain controller to ensure appropriate authentication of users that access secure resources on a remote server.

Directions

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 paste your lab screenshots in it.
3. Take the following screenshots during the lab:

- Section 1:
  - Part 1, Step 16.
  - Part 2, Step 21.
  - Part 3, Step 20.
  - Part 4, Step 12.
- Section 2:
  - Part 1, Step 7.
  - Part 2, Steps 4, 6.

- Part 3, Steps 4, 14.
- Part 4, Step 4.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template
IAS5025: Operating System Defense [Custom online lab bundle]

u02a1 - Presentation: Implementing Active Directory for Access Control

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Scenario

Imagine you are a member of the network security team at Widget Corp tasked with clarifying the potential advantages of deploying Active Directory and the company's enterprise information infrastructure. Widget Corp's current network is characterized by the following context:

- Widget Corp has decided to deploy a new ERP system.
- End-users will access the ERP system from 36 new workstations to be installed on the factory floor.
- The ERP system will be integrated with a number of SQL servers, file servers, and IIS servers each hosted on Windows Server 2016 computers.
- Widget Corp's support staff will continue to use a large installed base of legacy Windows workstations configured into multiple workgroups, including engineering, warehousing, and sales.

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.

Directions

Lab Documentation

Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template. Be specific. ***Note:****You only need to fill out the Lab Screenshots and Narrative section of the template.*

Presentation: Implementing Active Directory for Access Control

Prepare and record a 5–7 minute presentation (with voice and supporting visuals) with content and tone appropriate for IT professionals. It should describe specifics of the implementation Active Directory from a system administrator perspective.

Do the following:

- Explain the steps necessary to migrate from a Windows workgroup network to an Active Directory domain-based network.
- Explain how upgrading from a Windows workgroup to Active directory might impact the current users on a local machine.
- Explain how Active Directory implements access controls differently than a Windows workgroup.
- Suggest a strategy to correct disparate levels of user access when migrating to Active Directory.

Submission Requirements

Submit the following:

- Word document with your screenshots and explanation.
- Presentation file (if the file exceeds 15 MB, it should be compressed).

This week you will:

- Harden user accounts on a Linux system in a virtual lab.
- Explore managing and maintaining Linux OS security.

Unit 3 begins your exploration of specific steps available to secure Linux operating systems by using its built-in security features. Concepts related to the deployment of permissions based on users and groups are covered in the context of the principle of least privilege. Studies address the role of the shadow password suite in protecting the confidentiality, integrity, and availability of enterprise data.

Learning Activities

u03s1 - Studies

Readings

Read the following in your *Security Strategies in Linux Platforms and Applications* text to learn about Linux privileges and permissions:

- Chapter 4, "User Privileges and Permissions," pages 74–102.

Read the following in the Capella Library:

- Kundu, A., & Bano, P. (2015). SELinux & Linux repository: Introduction. *International Journal of Advanced Research in Computer Science, 6*(2).
    - This paper focuses on recent developments in Linux and the tools available to enhance Linux security.
- Pathak, N., & Sharma, N. (2018). Object oriented secure modeling using SELinux trusted operating system. *International Journal of Advanced Networking and Applications, 9*(4), 3492–3497.
    - This article explores the role of SELinux to achieve high security in web applications.
- Weinberger, M. (2015). The world of containers doesn't end with Docker. *Computerworld Digital Magazine, 1*(7), 3–5.
    - This article compares Docker to App Armor and SELinux and addresses their respective security functions.
- Venafi, Inc. researchers submit patent application, "System for managing cryptographic keys and trust relationships in a secure shell (ssh) environment," for approval. (2014, Nov 13). *Computer Weekly News*.
    - This article explores the management of public-private key pairs in an SSH environment.

Skillsoft Resources

View the following:

- Lachance, D. (2017). UNIX Essentials: Enabling SSH Public Key Authentication [Video]. Skillsoft, Ireland.

- Identify features and uses of access control tools.
- Explain features and applications for SELinux and App Armor.
- Identify and explain a third-party access control tools.

u03d1 - Linux Risks and Vulnerabilities

Based on your own personal or professional experience, or other exploration, consider methods by which Linux operating systems may be compromised through various vulnerabilities and security solutions used to mitigate those vulnerabilities.

Discuss one of the following:

- An attack vector created by unprotected or misconfigured Linux computers.
- A security vulnerability associated with running a specific daemon.
- The benefits of deploying SSH key-based authentication on Linux computers.

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 - Jones & Bartlett Lab: Hardening Security with User Account Management and Security Controls

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.

Overview

This week's hands-on lab provides you with an opportunity to define a password policy to secure user accounts in a Linux environment. You will learn how to organize users into groups to maximize access control to enterprise information resources. You will also learn to automate an account deletion procedure.

Directions

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 from Section 1:
    - Section 1:
        - Part 1, Step 9.
        - Part 3, Step 12.
        - Part 4, Step 12.
        - Part 5, Step 6.
    - Section 2:
        - Part 1, Step 6.
        - Part 2, Step 6.
        - Part 3, Step 5.
        - Part 4, Step 6.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template
IAS5025: Operating System Defense [Custom online lab bundle]

u03a1 - Hardening Security by Controlling Access

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Scenario

First World Bank Savings and Loan provides general information about its banking services to its customers from a public-facing Linux Web server. Customers may complete Web forms to request further information or to make an appointment with a banking specialist.

To ensure that the open nature of these customer interactions do not enable a disclosure of nonpublic personal information (NPI) on the server, First World requires layered security for its public-facing Web server. Following a recent data breach, the Bank's chief information officer (CIO), Frank Grandview, hired a consultant who recommended that the company institute a mandatory access control (MAC) policy as part of a defense-in-depth strategy.

Mr. Grandview wants to make sure that this is a sound strategy. Imagine he has asked you to compare the MAC solution to two other possible solutions - discretionary access control (DAC), and role-based access control (RBAC) just to be certain of the approach from a high level.

Imagine the choice is ultimately made to institute a MAC policy. He would like you to evaluate each and recommend one of the following:

- Security Enhanced Linux (SELinux).
- App Armor.
- A third party tool of your choosing.

Directions

Lab Documentation

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

Assignment: Memo - Recommendation to the CIO

Write a memo to the Bank's CIO that does the following:

- Compare and contrast mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC) authorization models.
- Based upon the information that you have, recommend which security solution to deploy and support it with compelling rationale. You will likely need to state assumptions regarding the First Bank Network that you need support your recommendation.

Submission Requirements

- Submit your assignment in a conventional memo format in the Assignment Template document below your lab documentation. Make sure to organize and label your responses clearly.

Unit 4 >> Securing Linux Services

Introduction

This week you will:

- Harden security by controlling network access to Linux system and iptables in a virtual lab.
- Discuss Linux service issues.

Unit 4 continues our exploration of layered Linux security with a focus on securing services. Concepts related to multitasking, user- and system-level processes, and daemons will be considered. Studies address some of the security vulnerabilities associated with various Linux services, and the risks they may pose to applications at runtime.

Learning Activities

u04s1 - Studies

Readings

Read the following in your *Security Strategies in Linux Platforms and Applications* text:

- Chapter 6, "Securing Services," pages 138–164.

Read following on the Capella Library:

- Hall, C. (2018). Microsoft brings Linux driven IoT security to Azure. *Windows IT Pro* (Online).
  - This article discusses Azure Cloud Switch, a Linux-based cross-platform operating system used for running data center switches and other network
- 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).
  - This article discusses SQL Injection attacks, which can pose a serious security threat to Web applications and web servers.
- Strom, D. (2016). 10 cutting-edge tools that take endpoint security to a new level. *Network World* (Online).
  - This article review a number of advanced endpoint detection and response tools for Linux systems.

Read the following on the Internet:

- Sciberras, N. (2014). Configuring your Web server to not disclose its identity. Retrieved from https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/

u04s1 - Learning Components

- Explain how a configuration file works.
- Understand how web server signatures may reveal vulnerabilities to attackers.
- Explain how to address server signature vulnerabilities..
- Understand how to identify server configuration issues that lead to security vulnerabilities.

- Understanding of server signature testing.

u04d1 - Linux Service Issues

Linux system administrators need to be concerned with system security, and to understand the risks to, and vulnerabilities of, the systems for which they are responsible. Based on your own personal or professional experience, or other exploration, discuss a particular security issue or vulnerability related to a Linux service and explore its implications with regard to confidentiality, integrity, or availability of enterprise data.

Discuss specific administrative or technical security controls that may effectively mitigate the issue or vulnerability. Some areas for you to consider may include:

- Absence of hardened systems.
- Legacy third-party applications.
- Nonexistence of data backups.
- Ineffective enforcement of password policies.
- Poor Linux operating system patch management.

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 - Jones & Bartlett Lab: Hardening Security for Linux Services and Applications

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.

Overview

This week's hands-on lab provides you with an opportunity to support the confidentiality, integrity, and availability of enterprise data by hardening Linux-based services and application. You will secure an open source web service, an

open source database application, and an open source email application. You will learn to deploy Secure Shell (SSH) to encrypt data in transit from a remote computer.

Directions

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 12, 20.
        - Part 2 Steps 8, 13.
        - Part 3 Step 7.
        - Part 4 Steps 19, 23.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template
IAS5025: Operating System Defense [Custom online lab bundle]

u04a1 - Hardening Security with User Account Management and Security Controls

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

Web server fingerprinting is an important task for network and system security administrators. Discovering the precise version and type of a production web server enables IT security auditors to determine known vulnerabilities and the potential exploits to use during penetration testing.

Preparation

View the Server Signature Test Result screenshot in the Resources and use it to answer the related question below.

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 Section 2 of this week's lab, you disabled the ServerSignature option in the Apache2 configuration file. Analyze how this configuration change serves to harden the security of a Linux server.
3. View the screenshot of the Signature Server Test Result. Identify the specific vulnerability being reported and suggest a specific server configuration change to correct the vulnerability.

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

Course Resources
Server Signature Test Result

Unit 5 >> Microsoft Windows Group Policy Control

Introduction

The week you will:

- Manage Group Policy within a Microsoft Windows computing environment in a virtual lab.
- Discuss password policies.

Unit 5 continues our exploration of methods for managing and maintaining Microsoft Windows security with a particular focus on the deployment of Group Policy and Group Policy Objects to enforce enterprise security policies. You will examine how Microsoft Windows uses Active Directory to centralize the enforcement of many security rules. Group Policy Objects are collections of Group Policy settings that can be easily applied to one or more users or computers. Maintenance of Group Policy and GPOs is considered, as are basic approaches for designing GPOs that align with an enterprise's security policy.

Learning Activities

u05s1 - Studies

Readings

Read the following in the Capella Library:

- Read the following in your *Security Strategies in Windows Platforms and Applications* text:
  - Chapter 6, "Group Policy Control in Microsoft Windows," pages 110–134.

Skillsoft Resources

View the following videos:

- Sampson, A. (2017). CompTIA Network+ N10-007: Password Policy [Video]. Skillsoft, Ireland.
  - After watching this video, you will be able to recognize appropriate password policies.
- Lachance, D. (2016). Windows Server 2016 - Identity: Password policy settings [Video]. Skillsoft, Ireland.
  - After watching this video, you will be able to configure domain and local user password policy setting.

u05s1 - Learning Components

- Explain elements of an audit policy.
- Recognize appropriate password policies.
- Understand hot to configure domain and local audit policy settings,

u05d1 - Password Policies

Consider your own personal or professional experience at a current or former employer, or other exploration, of using an enterprise computing environment.

Discuss the following:

- The current parameters of a specific enterprise's password policy and account lockout policy.
- An analysis of the degree to which these policy parameters align with best practices given the mission and other characteristics of the organization.

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

u05d1 - Learning Components

- Recognize appropriate password policies.

u05v1 - Jones & Bartlett Lab: Managing Group Policy within the Microsoft Windows Environment

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.

Overview

This week's hands-on lab provides you with an opportunity to work with Group Policy Objects (GPOs) in an Active Directory (AD) environment by deploying the Group Policy Manager Console (GPMC) to enforce enterprise security policies. You will use the command line interface to create security policy audit reports to verify the appropriate use of GPOs.

Directions

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 17.
        - Part 2, Step 10.
    - Section 2:
        - Part 1, Steps 5, 8, 16.
        - Part 2, Step 5.

Jones & Bartlett Technical Support

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

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

Course Resources

Assignment Template

IAS5025: Operating System Defense [Custom online lab bundle]

u05a1 - Managing Group Policy within the Microsoft Windows Environment

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

It is common for enterprise system administrators to manage Windows system security with Group Policy controls and Microsoft Baseline Security Analyzer (MBSA). However, MBSA has reached legacy status, and is no longer being supported by Microsoft. For this assignment you evaluate an audit policy, and research and review system security auditing tools that are appropriate for use in performing security audits of Windows 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.

- Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.
- Return to the Managing Group Policy within the Microsoft Windows lab. Using either the Group Policy Management Editor (GPME) or PowerShell, Examine the current Audit Policy settings, and suggest three changes to the existing audit policy that will strengthen the security of the domain, and explain your rationale for each change.

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

Unit 6 >> Auditing Microsoft Windows Security

Introduction

This week you will:

- Harden Windows server security using Microsoft Baseline Security Analyzer (MBSA) in a virtual lab.
- Discuss a Windows security breach.

Unit 6 continues our exploration of methods for managing and maintaining Microsoft Windows security with a particular focus on auditing the security of Windows machines in support of protecting the confidentiality, integrity, and availability of enterprise data. You learn how to analyze a computer's configuration to ensure that security controls are appropriately working to enforce organizational security policies, and to correct settings that do not conform to best practices.

Learning Activities

u06s1 - Studies

Readings

Read the following in the Capella Library:

- Read the following in your *Security Strategies in Windows Platforms and Applications* text:
  - Chapter 7, "Microsoft Windows Security Profile and Audit Tools," pages 135–161.

Read following on the Internet:

- Keary, T. (2018). 6 Best Alternatives to Microsoft Baseline Security Analyzer. Retrieved from https://www.comparitech.com/net-admin/alternatives-to-microsoft-baseline-security-analyzer/
  - This article discusses a number of server security auditing tools that have advanced capabilities relative to Microsoft Baseline Security Analyzer

Skillsoft Resources

View the following video:

- Welton. T. (2015). Microsoft Security Fundamentals: Microsoft Baseline Security Analyzer (MBSA) [Video]. Skillsoft, Ireland.

Optional Reading

- Microsoft. (2017). Windows Server 2016 security: Better protection begins at the OS [PDF]. Retrieved from: http://download.microsoft.com/download/6/7/3/673E651E-C5B3-4C93-A69A-94042EB6DE22/Windows_Server_2016_Security_Better_protection_begins_at_the_OS_Whitepaper_EN_US.pdf
  - This white paper addresses best practices for actively defending Windows Server 2016 computers.

u06s1 - Learning Components

- Describe the features of Microsoft’s Group Policy Management tool.
- Describe the features of Microsoft’s Policy Analyzer tool.
- Identify features and applications for Windows system security authoring tools.

u06d1 - Window Security Breach

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

Discuss the following:

- The attack vectors and techniques used to carry out the attack.
- The possible motivations of the attacker.
- How the incident was detected, and the steps taken to mitigate its effects.
- How proactive security auditing 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 - Jones & Bartlett Lab: Hardening Windows Server Security Using Microsoft Baseline Security Analyzer

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.

Overview

This week's hands-on lab provides you with an opportunity to deploy the Windows Event Viewer utility to search for evidence of unauthorized access to enterprise data resources. You will also launch an attack against a Windows server and study the logs to identify an attack vector and recommend appropriate risk mitigation.

Directions

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 33.
- Section 2:
  - Part 1, Steps 13, 19.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template
IAS5025: Operating System Defense [Custom online lab bundle]

u06a1 - Server Security Auditing Tools

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

Security administrators routinely deploy tools to monitor, analyze, and audit operating system security on enterprise workstations and servers as part of a proactive defense-in-depth strategy.

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.

Lab Related Assignment

In this week's lab, you explored the GPO report generated by the Group Policy Management tool and the Policy Analyzer created from the registry information.

1. Briefly describe what you learned from or observed in the lab and include it in the section with your screenshots in the Assignment Template found in the Resources. Be specific.
2. Explain which tool used in the lab is more appropriate for making changes to a single policy or group of policies.

3. Explain which tool used in the lab is better suited to verifying a large number of policy changes at once.

Windows Security Audit Tools

It is common for enterprise system administrators to manage Windows system security with Group Policy controls and Microsoft Baseline Security Analyzer (MBSA). However, MBSA has reached legacy status, and is no longer being supported by Microsoft. Research and review system security auditing tools that are appropriate for use in performing security audits of Windows servers.

1. Compare and contrast three system security auditing tools that are appropriate for use in performing security audits of Windows servers. Make sure to identify specific features that distinguish them from one another.
2. Explain what your biggest consideration in choosing one of these tools. State any assumptions you need to make.

Unit 7 >> Linux-Based Firewalls

Introduction

This week you will:

- Configure host-based IP firewall services in a virtual lab.
- Discuss host-based and network-based firewall deployment.

Unit 7 continues our exploration of layered Linux security with a focus on securing network connections using host-based Linux firewalls. Concepts related to access control lists (ACLs), TCP Wrapper, and iptables will be addressed. Studies will extend understanding of the functions and features of Security Enhanced Linux (SELinux) and Application Armor (AppArmor).

Learning Activities

u07s1 - Studies

Readings

Read the following in your *Security Strategies in Linux Platforms and Applications* text:

- Chapter 7, "Networks, Firewalls, and More," pages 166–209.

Read following on the Internet:

- Firewalld.org. (2018). How to. Retrieved from https://firewalld.org/documentation/howto/
  - This resource provides how to information regarding enabling and disabling firewalld, get firewalld state, reload firewalld, open a port or service, add a service, and debug firewalld.

- Anicas, M. (2015). Iptables Essentials: Common Firewall Rules and Commands. Retrieved from https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands
    - This article provides a quick reference to iptables commands used to create common firewall rules.

Skillsoft Resources

View the following:

- Lachance, D. (2015). RHEL 7: Adding or Deleting an iptable Rule [Video]. Skillsoft, Ireland.
    - After watching this video, you will be able to add and delete rules to an iptable configured firewall.
- Lachance, D. (2015). RHEL 7: Saving and Restoring iptable Rulesets [Video]. Skillsoft, Ireland.
    - After watching this video, you will be able to save and restore iptable rulesets.
- Lachance, D. (2015). RHEL 7: Describing iptable Rules and Configuration [Video]. Skillsoft, Ireland.
    - After watching this video, you will be able to describe the sections of the firewall and the basics of how the firewall rules are configured.

u07s1 - Learning Components

- Understand methods of firewall filtering.
- Identify firewalld and iptables feature sets.
- Understand how FirewallD can deny requests.
- Understand the role and functioning of TCP and UDP ports.

u07v1 - Jones & Bartlett Lab: Hardening Security by Controlling Access

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.

Overview

This week's hands-on lab provides you with an opportunity to create and deploy a firewall rule set that significantly restricts access to network resources. You will use a host-based access control system to filter access to networked servers. You will deploy a Linux kernel security module that serves as a mechanism for enforcing access control policies.

Directions

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, 13.
  - Part 2, Step 14.
  - Part 3, Steps 3, 5, 14.
- Section 2:
  - Part 1, Step 20.
  - Part 2, Step 12.
  - Part 3, Step 5.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template
IAS5025: Operating System Defense [Custom online lab bundle]

u07a1 - Configure a Linux-Based Firewall

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

This week you learned about the role of firewalls in protecting Linux workstations and servers by explicitly permitting or denying traffic based on specific attributes. In this assignment you will build on your lab experience by further exploring the functions and features of iptables and firewalld, and then you will return to the lab to complete a self-directed hands-on challenge.

Preparation

- Use the Internet to research differences between iptables and firewalld.
- Use the Internet to determine how to drop ICMP requests using firewalld on the TargetLinux01 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.

Part 1:

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 firewalld's zones and services to iptables chain rules.
3. Recommend a specific firewall as your preference for deployment in an enterprise that requires the highest levels of information security, and include your rationale for that preference. Please be sure to properly cite applicable resources.

Part 2: Return to the Lab

Return to this week's Lab: "Hardening Security by Controlling Access," and do the following:

1. Use the Internet to determine how to deny ICMP requests using firewalld on the TargetLinux01 machine. Implement the changes, then reload the firewall rules and submit a Ping request from the vWorkstation. Take a screenshot showing the results of the Ping test. Describe how it works.
2. In Section 2, you edited the hosts.deny file to prohibit SSH traffic from all sources except the vWorkstation. Edit the /etc/hosts.allow file to specify allow SSH traffic from the vWorkstation and log successful connections from that host, and test the configuration. Take a screenshot of the /var/log/tcpwrapper.log file showing the successful connections. Describe how the file works to control traffic.

Submission Requirements

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

u07d1 - Host-Based and Network-Based Firewall Deployment

Enterprises of all sizes need to secure proprietary, regulated, or mission-critical data on networked servers, workstations, and other devices that are connected to the Internet. Consider your own personal or professional experience, or other exploration, of using or administering firewall systems.

Discuss the following:

- Advantages and disadvantages of host-based firewalls.
- Advantages and disadvantages of network-based firewalls.
- Describe a situation where a combination of both host-based and network-based solutions may be well worth the expense, administrative overhead, and added network design complexity.

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

u07d1 - Learning Components

- Understand methods of firewall filtering.

Unit 8 >> Mobile OS Security

Introduction

This week you will:

- Harden security for a Linux kernel in a virtual lab.
- Create a written Mobile Device Management (MDM) deployment plan.
- Explore concepts and issues related to mobile device security.

Securing mobile operating systems is critical for enterprises that rely on mobile computing devices, including smartphones, to support the productivity of their employees. Many organizations embrace the 'bring your own device' (BYOD) trend, which enables workers to use their personal mobile smartphones, and other mobile computing devices, to access enterprise data and business process applications.

Learning Activities

u08s1 - Studies

Readings

Read the following in your *Security Strategies in Linux Platforms and Applications* text:

- Chapter 10, "Kernel Security Risk Mitigation," pages 278–309.

Read the following in the Capella Library:

- Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22(1), 97–114.
    - This paper examines mobile device security in the context of small- to medium-sized enterprises who use mobile devices as part of their mobility business strategy.

- Jasek, R. (2015). Security deficiencies in the architecture and overview of Android and iOS mobile operating systems. Paper presented at the International Conference on Cyber Warfare and Security,153–X.
    - This article presents an overview of the Android and iOS mobile operating systems from a security standpoint, selected on the basis of their opposing approaches to openness and any third-party customizations that users are allowed to perform.
- Kuļešovs, I., Borzovs, J., Susters, A., Arnicane, V., Arnicans, G., Keiduns, K., & Skutelis, J. (2018). An approach for iOS applications' testing. *Baltic Journal of Modern Computing, 6*(1), 56–91.
    - The study discusses Apple iOS security capabilities and risks.
- Yuksel, A. S., Zaim, A. H., & Aydin, M. A. (2014). A comprehensive analysis of Android security and proposed solutions. *International Journal of Computer Network and Information Security*, 6(12), 9–20.
    - This article presents the taxonomy of Android-based mobile security solutions.

Skillsoft Resources

Read the following:

- Doherty, J. *Wireless and mobile device security* (1st ed.). Burlington, MA: Jones & Bartlett Learning.
    - Chapter 11, "Mobile Communication Security Challenges," pages 246–262.

View the following:

- Lachance, D. (2015). CompTIA Mobility+: Mobile Device Management [Video]. Skillsoft, Ireland.
    - This video provides an overview on how to administer mobile devices using an MDM solution for CompTIA's Mobility+ certification.
- Lachance, D. (2015). Security Trends: Mobile Devices and Malware [Video]. Skillsoft, Ireland.
    - After watching this video, you will be able to describe how the prevalence of mobile devices has created a whole new platform for vulnerabilities.

u08s1 - Learning Components

- Explain how MDM features are related to levels of security.
- Understand MDM functions and features.
- Explain how MDM systems work to provide mobile device security.
- Understand options for cloud-based MDM.
- Understand the functions of smartphone operating systems that integrate with MDM.

u08d1 - Security Breaches of Mobile Devices

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

Discuss the following:

- Attack vectors and techniques use to carry out the attack.
- Probable motivation of the attacker.
- How the incident was detected.
- Mobile OS security controls that may 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

u08v1 - Jones & Bartlett Lab: Hardening Security for the Linux Kernel

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.

Overview

This week's hands-on lab provides you with an opportunity to harden a Linux kernel. You will analyze specific configuration files and revise them to reconfigure system settings. You will learn how to access a list that indicates the status of modules running in the Linux kernel.

Directions

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 9, 13.
        - Part 2, Step 7.
        - Part 3, Steps 3, 5, 7, 9.
        - Part 4, Step 6.
    - Section 2:

- Part 1, Steps 14, 19, 23.
- Part 2, Step 8.
- Part 3, Step 2.
- Part 4, Steps 3, 10.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template
IAS5025: Operating System Defense [Custom online lab bundle]

u08a1 - Hardening Security for the Linux Kernel

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

Mobility is often crucial to the productivity of an enterprise's workforce. Mobile Device Management (MDM) systems, both on premise and cloud-based, are emerging as a robust component of many enterprise information technology infrastructures because they enable security administrators to manage mobile endpoints from a central location.

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.

Lab Related Documentation

1. Describe briefly what you learned or observed in the lab and include it in the section with your screenshots. Be specific.

Non-Lab Assignment: First World Bank Scenario

Consider the scenario:

First World Bank Savings and Loan has decided to deploy a bring-your-own-device (BYOD) strategy to allow its employees to use their personal smartphones to access the Bank's data instead of using smartphones provided by the company. The information technology (IT) department needs to manage the mobile operating system on BYOD devices to protect the confidentiality and integrity of sensitive information. You have been tasked by the Bank's CIO to report on third-party Mobile Device Management (MDM) solutions, and to make a specific recommendation for the Bank to deploy.

Write 3-4 pages that do the following:

- Identifies and describes three of the most important MDM systems features that meet the bank's need for extremely high security.
- Compare the feature sets of three commercial MDM solutions, including at least one cloud-based solution, and make a specific MDM solution recommendation for the bank to deploy.
- Describe the functional relationship between your recommended MDM solution and a smart phone (your choice) native operating system.

Submission Requirements

- Length of report: 3-4 double-space pages, excluding the references page.
- Font: Times New Roman, 12 point.
- Formatting: Resources and citations are formatted according to current APA style.

Unit 9 >> Microsoft Windows Application Security

Introduction

This week you will:

- Identify security hardening opportunities for Microsoft's Internet Information Services (IIS) web server application and the Internet Explorer web browser in a virtual lab.
- Discuss a Windows zero-day attack.

This unit focuses on best practices for hardening Windows applications with the goal of protecting the confidentiality, integrity, and availability of enterprise data. You will examine and apply the principles of Microsoft application security to ensure the secure configuration of client and server applications. Consideration is given to case studies which demonstrate the application of best practices for securing applications in a Windows environment.

Learning Activities

u09s1 - Studies

Readings

Read the following in the Capella Library:

- Read the following in your *Security Strategies in Windows Platforms and Applications* text:
  - Chapter 12, "Microsoft Application Security," pages 279–303.
- Joh, H. & Malaiya, Y. K. (2017). Periodicity in software vulnerability discovery, patching and exploitation. *International Journal of Information Security, 16*(6), 673–690.
  - This article addresses key processes related to software vulnerabilities that need to be taken into account for assessing security at a given time.
- Morimoto, R. (2017). Top 5 Windows Server 2016 features that enterprises are deploying. *Network World* (Online).
  - This article focuses on organizations that intend to deploy an integrated roll-up of various Windows Server services with solutions intended to provide high availability
- Rashid, F. Y. (2016). Lockdown! Harden Windows 10 for maximum security. *InfoWorld.com*.
  - This article discusses Windows 10 cryptographic features.

Read the following on the Internet:

- Ohlinger, M. (2014). How to create a Windows Firewall Inbound Rule. Retrieved from https://blogs.msdn.microsoft.com/mandi/2014/11/03/how-to-create-a-windows-firewall-inbound-rule/
  - This article details the steps to allow connections on TCP port 8080 using Windows Firewall.

Skillsoft Resources

- Lachance, D. (2014). CompTIA Cloud+: Changing the Attack Surface [Video]. Skillsoft, Ireland.
  - This video provides an overview on how to harden a Windows computer by reducing its surface vulnerability.
- Lachance, D. (2015). CompTIA Cloud+: Host Hardening [Video]. Skillsoft, Ireland.
  - This video provides an overview on how to implement host hardening.
- Hendry, B. (2018). Team Foundation Server 2017: Internet Explorer Enhanced Security Configuration [Video]. Skillsoft, Ireland.
  - After watching this video, you will be able to configure security in Internet Explorer.
- Yates, J. (2015). Windows 10: Countermeasures [Video]. Skillsoft, Ireland.
  - After watching this video, you will be able to describe countermeasures.

Consider your own personal or professional experience, or other exploration, of making a Microsoft Windows computer more secure. Discuss each of the following:

- Specific methods or steps that you have taken to harden a Windows computer.
- A recent news story, or career anecdote, regarding a zero-day exploit against Windows.
- Recommended actions to repel or mitigate a zero-day 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

u09v1 - Jones & Bartlett Lab: Securing Internet Client and Server Applications on Windows Systems

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.

Overview

This week's hands-on lab provides you with an opportunity to harden a Windows-based Web service and a proprietary browser application. You will create appropriate documentation of server configuration changes, and explore how each specific change works to support the confidentiality, integrity, and availability of enterprise data.

Directions

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 31.
        - Part 2, Steps 8, 21.
    - Section 2:

- Part 1, Step 9.
- Part 2, Steps 8, 11.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template
IAS5025: Operating System Defense [Custom online lab bundle]

u09a1 - Securing Internet Client and Server Applications on Windows Systems

By now you should have completed the unit lab and saved your screenshots to a Word document for submission with this assignment.

Overview

For this assignment you'll need to explore specific measure to harden Web browsers. You will also have an opportunity to revisit the virtual lab environment to modify the TCP port number used for http traffic.

Preparation

Use the Internet or the Capella University Library to research:

- Hardening recommendations for your chosen Internet browser.
- Uses for port 8080 in Windows Server 2016 IIS.

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 why there are so few steps to securing a default installation of Internet Information Services (IIS) in Windows Server 2016 as compared with legacy systems.

3. Recommend three hardening measures to improve the security of your chosen Internet browser.
4. Return to the unit lab, "Securing Internet Client and Server Applications on Windows Systems," and do the following:
    - In IIS, change the default port number for the Default Web Page from 80 to 8080. Take a screenshot showing the change, and explain its implications.

Submission Requirements

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

Unit 10 >> Cloud-based Operating Systems Security

Introduction

This week you will:

- Explore cloud-based security considerations.
- Discuss OS security in cloud-based infrastructures.
- Reflect upon what you learned in the course.

In this final unit of the course we will turn our attention to thinking about the future of operating system security, particularly as it relates to cloud computing, virtualization, and infrastructure as a service (IaaS) environments. You also reflect on your learning in this course, and assess its impact on your information technology career opportunities and on the job performance.

Learning Activities

u10s1 - Studies

Readings

Read following on the Internet:

- Kazim, Muhammad & Masood, Rahat & Shibli, Awais. (2013). Security Aspects of Virtualization in Cloud Computing. Retrieved from https://www.researchgate.net/publication/273950406_Security_Aspects_of_Virtualization_in_Cloud_Computing
    - In this paper, different aspects of cloud virtualization security are explored.

Skillsoft Resources

Read the following:

- Vacca, J. R. (2017). *Security in the private cloud.* CRC Press.
  - Chapter 3, "Infrastructure as a service," pages 37–46.
- Samani, R., Honan, B., & Reavis, J. (2015). *CSA guide to cloud computing: Implementing cloud privacy and security.* Syngress Publishing.
  - Chapter 3, "The Cloud Threat Landscape," pages 35–59.
- Rountree, D. & Castrillo, I. (2014). *The basics of cloud computing: Understanding the fundamentals of cloud computing in theory and practice.* Syngress Publishing.
  - Chapter 6 , "Evaluating Cloud Security—An Information Security Framework," pages 101–119.

View the following:

- Lachance, D. (2015). Cloud Computing Technology Fundamentals: Cloud Network Infrastructure Security [Video]. Skillsoft, Ireland.
  - After watching this video, you will be able to describe considerations for infrastructure security in cloud computing.

u10d1 - Operating Systems Security in Cloud-Based Infrastructures

It is often necessary for information technologists to evaluate new and emerging technologies and to assess the potential impacts on an enterprise's current information technology (IT) security operations. Discuss issues related to operating system security in the context of cloud-based network infrastructures. Speak from your own personal or professional experience, or research the following topics to inform your viewpoint:

- Ways in which the role of operation systems may change in a cloud computing environment.
- Best practices for security operating systems on virtual machines and the physical machines that host them.
- Operating systems security risks and vulnerabilities that may be unique to cloud computing environments.
- Operating system defenses to deploy and an IaaS cloud 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

u10d2 - Course Reflection

Share the aspects of this course that you found most useful to your career aspirations, and describe how the knowledge and skills that you learned may enhance your professional performance. Responses to peers are not required.

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide