Preview: IAS5211 : Mobile and Wireless Network Architecture and Security

Syllabus

Course Overview

Course Overview

This course provides you with both practical and theoretical aspects of the core concepts, technologies, components, and security issues related to mobile and wireless networks. This course includes hands-on labs where you have the opportunity to apply network defense tools to identify and mitigate mobile network security concerns and apply network defense tools to identify and mitigate wireless security concerns. You will evaluate approaches to digital communication and analyze how mobile systems operate to facilitate secure access and voice, and examine wireless and mobile network principles, architectures, and protocols.

Assignments

Week 1: Lab: Ethical Hacking: Performing passive reconnaissance on a target organization. 12% of grade. *Scoring Guide*

Week 2: 4G LTE Security for Mobile Network Operators. 8% of grade. *Scoring Guide*

Week 4: Bring Your Own Device: Security Implications. 8% of grade. *Scoring Guide*

Week 5: Lab: Conducting Scanning and Enumeration on a Target Network. 12% of grade. *Scoring Guide*

Week 6: IoT Network Security in a Healthcare Environment. 8% of grade. *Scoring Guide*

Week 7: Lab: Auditing a Wireless Network and Planning for a Secure WLAN Implementation. 12 % of grade. *Scoring Guide*

Week 8: Wireless Sensor Networks: Threats and Mitigation. 8% of grade. *Scoring Guide*

Week 9: **Lab:** Ethical Hacking: Performing Post-exploitation Activities and Evasive Maneuvers. 12% of grade. *Scoring Guide*

Discussions

There will be a discussion each week that will help you understand and organize concepts to help you with the hands-on labs and assignments. Participation in discussions will count for 20% of your final grade.

Week 1: 1G to 5G Architecture Evolution

Week 3: Hands-on Personal Mobile Device Security and Privacy

Week 9: Risks to Your Home Wireless Network

Week 10: Analyzing security of RFID implementation for Warehouse and Inventory Management

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

Course Competencies

(Read Only)

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

1. Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.
2. Compare and contrast different approaches to digital communication.
3. Analyze how mobile systems operate to facilitate secure data access and voice.
4. Apply network defense tools to identify and mitigate mobile network security concerns.
5. Apply network defense tools to identify and mitigate wireless security concerns.
6. Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.

Course Prerequisites

There are no prerequisites for this course.

Syllabus >> Course Materials

Required

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

Integrated Materials

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

Book

Capella University (Ed.). (2020). *IAS5211: Mobile and wireless network architecture and security* [Custom online lab bundle]. Burlington, MA: Jones & Bartlett. ISBN: 9781284210118.

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.

- Adăscăliţei, I. (2019). Smartphones and IoT security. *Informatica Economica, 23*(2), 63–71.
- Baillette, P., Barlette, Y., & Leeclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end-users. *International Journal of Information Management, 43*, 76–84.
- Biswal, A. K., Jenamani, M., & Kumar, S. K. (2018). Warehouse efficiency improvement using RFID in a humanitarian supply chain: Implications for Indian food security system. *Transportation Research Part E: Logistics and Transportation Review, 109*, 205–224.
- Burhan, M., Rehman, R. A., Khan, B., & Byung-Seo, K. (2018). IoT Elements, layered architectures, and security issues: A comprehensive survey. *Sensors, 18*(9).
- Chandramouli, D., Liebhart, R., & Pirskanen, J. (2019). *5G for the connected world* (1st ed.). Hoboken, NJ: John Wiley & Sons, Inc.
- Deebak, B. D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2019). An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. IEEE Access, 7, 135632–135649.
- Eluwole, O. T., Udoh, N., Ojo, M., Okoro, C., & Akinyoade, A. J. (2018). From 1G to 5G, What next? *IAENG International Journal of Computer Science, 45*(3), 1–22.
- Fang, D. (2019). Efficient and flexible solutions for 5G wireless network security. Dissertation (ProQuest).
- Gökçe, K. G., & Doerlioglu, O. (2019). "Bring your own device" policies: Perspective of both employees and organizations. *Knowledge Management & E-Learning, 11*(2), 233–246.
- Kalniņš, R., Puriņš, J., & Alksnis, G. (2017). Security evaluation of wireless network access points. *Applied Computer Systems, 21*(1), 38–45.
- Lachance, D. (2015). *Systems security certified practitioner: Wireless transmission security.* [Video] Skillsoft Ireland.
- Lorenzo, S. F., Benito, J. A., Cardarelli, P. G., Garaia, J. A., & Juaristi, S. A. (2019). A comprehensive review of RFID and Bluetooth security: Practical analysis. *Technologies, 7*(1), 15.
- Moran, J. (n.d.) *CompTIA Security+ SY0-501: Wireless security settings* [COURSE]. Skillsoft.
- Onasanya, A., Lakkis, S., & Elshakankiri, M. (2019). Implementing IoT/WSN based smart Saskatchewan Healthcare System. *Wireless Networks, 25*(7), 3999–4020.
- Shannon, M. (2016). *CISA: Wireless security threats and mitigation* [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). *Certified ethical hacker - CEHv10: Wireless hacking common threats.* [Course]. Skillsoft Ireland Limited.
- Verkijika, S. F. (2019). If you know what to do, you will take action to avoid mobile phishing attacks: Self-efficacy, anticipated regret, and gender *Computers in Human Behavior, 101*, 28–296.
- Vijayalakshmi, S. R., & Muruganand, S. (2018). *Wireless sensor networks: An introduction.* Mercury Learning.
- Welton, T. (2015). *Internet of things: Additional IoT operating systems* [Video]. Skillsoft Ireland Limited.
- Welton, T. (2015). *Internet of things: Introduction to IoT operating systems* [Video]. Skillsoft Ireland Limited.
- Wong, V. W. S. (2017). *Key technologies for 5G wireless systems.* New York, NY, USA
- Yan, P., & Zheng, Y. (2018). A survey on dynamic mobile malware detection. *Software Quality Journal, 26*(3), 891–919.

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.

- Android.com. Secure an Android device. Retrieved from https://source.android.com/security
- Apple.com. You have control over what you share. Retrieved from https://www.apple.com/privacy/control/
- Bhasker, D. (2016). 4G LTE security for mobile network operators. *Journal of Cybersecurity and Information Systems 1*(4). Retrieved from https://www.csiac.org/journal-article/4g-lte-security-for-mobile-network-operators/7/
- GSMA.com. (2019). *Mobile telecommunications security threat landscape* [PDF]. Retrieved from https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf
- Gul, M. (2019). How to configure your IPhone for internet privacy and security. Retrieved from https://www.ilounge.com/articles/how-to-configure-your-iphone-for-internet-privacy-and-security
- Mansuri, S. (2019). Complete guide on RFID and its applications in supply chain management and logistics. Retrieved from https://www.peerbits.com/blog/rfid-applications-in-supply-chain-management-and-logistics.html
- Top10VPN.com. (2020). Top 10 best VPN services for USA. Retrieved from https://www.top10vpn.com/best-vpn-for-usa/?v=control&bsid=c33se1kw421&gclid=CjwKCAiA0svwBRBhEiwAHqKjFj6ltMcpQj7XRtewytJFj8B-nL5uDkeNE9FLRMFpnNF8osRg2xl-qhoCUaUQAvD_BwE
- U.S. Department of Homeland Security: CISA. (2019). Security tip (ST05-003) - Securing wireless networks. Retrieved from https://www.us-cert.gov

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.

Unit 1 >> Evolution of Telecommunications through 5G Mobile

Introduction

The Need to Protect Against Data Communication Security Threats

As we progress into the 5G era, it becomes possible to predict revenue generation in the trillions of dollars in the combined markets of media, telecommunications, and IT markets as mobile flexibility, high-speed multimedia, and Internet of Things (IoT) integrate to allow a wide range of new capabilities. Studies performed by key organizations in the telecom world suggest that by 2035 there will be over 20 million 5G-related jobs. The need to understand the evolution of mobile/cellular technologies that have led to 5G and the need to understand the 5G threat landscape and how to implement secure 5G technologies is critical to network defense students.

To-Do List

- **Prepare:** Become familiar with the technology and software resources used in the course including the labs and how you will incorporate the lab reports into the lab assignments.
- **Prepare:** Create a lab report as directed in the lab to incorporate into the assignment for this week.
- **Discussion:** Participate in a discussion to create a presentation to help the employees understand how the network architecture has evolved from 1G to 5G, and how this evolution has changed the threat environment and related security approaches across each of the generations.
- **Assignment:** Complete a hands-on lab and write an essay about performing passive reconnaissance on a target organization.
- **What You Need to Know:** Study the concepts, technologies, components, and security issues related to mobile networks.

Learning Activities

u01s1 - Activity Overviews

Discussion Overview

In the discussion for this week, you will create a presentation to help the employees understand how the network architecture has evolved from 1G to 5G, and how this evolution has changed the threat environment and related security approaches across each of the generations.

Assignment Overview

In this assignment for this week, you will complete a hands-on lab and write an essay about performing passive reconnaissance on a target organization.

u01s2 - What You Need to Know

The Evolution of Mobile Technology

The following resources provide information about the evolution of mobile technology and the current 5G technology.

- Eluwole, O. T., Udoh, N., Ojo, M., Okoro, C., & Akinyoade, A. J. (2018). From 1G to 5G, What next? *IAENG International Journal of Computer Science, 45*(3), 1–22.
    - This is an overview of the evolution of 1G to 5G technology and will be helpful to you in completing the discussion question.
- Chandramouli, D., Liebhart, R., & Pirskanen, J. (2019). *5G for the connected world* (1st ed.). Hoboken, NJ: John Wiley & Sons, Inc.
    - Chapter 1: Drivers and Motivation for 5G
    - Chapter 4: Next Generation Network Architecture
        - These chapters will be helpful to you in discussing next-generation network architecture and related security issues and mitigation.
- Wong, V. W. S. (2017). *Key technologies for 5G wireless systems.* New York, NY, USA.
    - Chapter 1: Overview of new technologies for 5G systems
    - This chapter will introduce you to new technologies that will make use of 5G architecture.

u01s3 - Prepare: Software and Technology Access

In this course, you will be using software and technology that is needed to complete designated activities and assignments. There is no additional cost for this software and technology. Some software packages will be made available to you at no additional cost through Capella's subscription with Microsoft, while other software packages are available for free download through open-source licensing.

If you use a Mac, refer to Installing a Virtual Windows Environment in the Tools and Resources section of the courseroom.

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

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

Microsoft Software

1. Visit Capella's Microsoft Software page for instructions on obtaining free Microsoft software.
2. Identify the version of MS Visio, Project, Access,Visual Studio Enterprise, or SQL Server, etc. that is compatible with your operating system.
3. Download and install.

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 some of the assignments.

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

Additional Online Resources

The course materials you have procured include an access code for additional online resources. Follow the instructions below.

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

u01s4 - Prepare: Lab activity and assignment

The first step in ethical hacking is reconnaissance, the stage where footprinting, scanning, and enumeration techniques are used to gather information about a target. That target can be a network, a computer, a server, an IoT device or network, or a mobile device or mobile network. An ethical hacker will gather as much core information as possible, understand the range of the network, identify all active devices, look for access points such as open ports, fingerprint any operating systems, identify services on ports, and map the overall network. Organizations that rely on Bring Your Own Device (BYOD) might have many vulnerabilities through employee mobile devices. In this lab, you will learn how to perform passive reconnaissance activities.

Your assignment, which is related to the lab will require that you provide pre-defined screenshots of various parts of the lab and write a two-paragraph summary of what you experienced and learned when completing the lab.

You will also be asked to discuss security threats in a BYOD environment, how passive reconnaissance might occur in that environment, and potential security controls to prevent this.

u01d1 - Write Your Discussion Post

1G to 5G Architecture Evolution

Read the discussion participation scoring guide to learn how the instructor will evaluate your discussion participation throughout the course. After reviewing the resources in What You Need to Know, respond to the following discussion topic.

As an IT and security expert, you have been asked to give a presentation to the IT and security employees of a mobile carrier service. They have asked that you help the employees understand how the network architecture has evolved from 1G to 5G, and how this evolution has changed the threat environment and related security approaches across each of the generations. Provide specific examples of a security threat and solution for each generation. Use information from this week's reading as well as research in Capella's library and on the Internet.

Create your response as a PowerPoint presentation that is a minimum of 10–12 slides.

In your presentation, use at least one of the assigned readings or audiovisual resources to support your points.

Response Guidelines

Read the posts of your peers and respond to two of them. How do your peers' opinions and results contrast with your own? Do you agree or disagree with the analysis of your peers? Explain.

Course Resources
Graduate Discussion Participation Scoring Guide

u01v1 - Hands-On Lab: Ethical Hacking: Performing Passive Reconnaissance on a Target Organization

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities. Be prepared to describe the following lab activities in the assignment for this week.

1. Use customized Google searches to perform focused vulnerability searches.
2. Use hacking tools to scrape information from public databases.
3. Query Internet registration authorities for domain information.
4. Use Maltego to identify publicly available e-mail addresses and domain names.

Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Lab report with screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

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

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

u01a1 - Lab: Ethical Hacking: Performing passive reconnaissance on a target organization

Overview

In this assignment, you will submit a 1–2-page essay that addresses the questions presented in this assignment and includes the lab report from the virtual lab for this week. You must complete the lab before completing this assignment.

Instructions

In your essay for this assignment describe the following activities you completed for the Performing Passive Reconnaissance on a Target Organization lab.

1. Use customized Google searches to perform focused vulnerability searches.
2. Use hacking tools to scrape information from public databases.
3. Query Internet registration authorities for domain information.

4. Use Maltego to identify publicly available e-mail addresses and domain names.

In your own words, describe what you learned from this lab on performing passive reconnaissance on a target organization.

Perform research on the Internet to understand security threats and attack vectors in a Bring Your Own Device (BYOD) scenario. How could passive reconnaissance be done in this type of environment? What security controls would you recommend implementing to avoid this type of passive reconnaissance?

Submit your essay including the lab report for this assignment by 11:59 pm on Sunday of this week.

Additional Requirements

- **Written communication:** Ensure written communication is free of errors that detract from the overall message.
- **Length of paper:** 1-2 typed, double-spaced essay pages, lab report pages, title page, and reference page.
- **Format**: Format resources and citations according to APA guidelines for style and format.
- **Font and font-size:** Use Times New Roman 12-point font.
- **Sources:** Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
  - Apply your internet research findings to analyze core concepts and applied technologies regarding security threats and attack vectors in a Bring Your Own Device (BYOD) context.
- **Competency 3: Analyze how mobile systems operate to facilitate secure data access and voice.**
  - Describe performing passive reconnaissance on a target organization in a lab context.
  - Recommend security controls to implement to avoid identified passive reconnaissance in a Bring Your Own Device (BYOD) context.
- **Competency 4: Apply network defense tools to identify and mitigate mobile network security concerns.**
  - Complete the lab tasks as described in the lab learning objectives.
  - Describe how passive reconnaissance can be applied in a Bring Your Own Device (BYOD) context.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Convey clear meaning through appropriate word choice and usage.
  - Organize content so ideas flow logically with smooth transitions.

Introduction

Protecting Mobile Networks

A Mobile Network Operator (MNO) is a wireless carrier or service provider, a cellular business or a mobile network carrier. An MNO must control or own access to a radio spectrum license from some government or regulatory agency. In addition, an MNO must also either control or own all aspects of the network infrastructure required to give subscriber services over the licensed spectrum. Examples of U.S. MNOs are AT&T, Verizon Wireless, and Sprint Corporation.

It is important to understand the concept of Long Term Evolution (LTE) which is a 4G wireless standard created by the 3rd Generation Partnership Project (3GPP). It is created to offer up to ten times the speeds of 3G networks for tablets, notebooks, smartphones, and wireless hotspots. LTE is complex and contains a number of security vulnerabilities. Consider that the LTE ecosystem included as of 2017, 569 million users across 87 countries. There are over 821 forms of user equipment and a wide range of content service providers and applications available. Additionally, there were, as of 2017, 248 commercial LTE deployments and over 415 Mobile Network Operators (MNOs), as well as 97 device manufacturers.

For the MNO, there are many layers of security vulnerabilities in existence which include interconnections to other MNOs, a wide range of security standards, insecure behaviors of end-user subscribers, and poor security in third-party services and application.

To-Do List

- **Assignment:** Create a PowerPoint presentation that describes identified threats to a mobile network, discusses the impact to businesses and to the mobile network operator of these threats, and recommendations for mitigating these threats.
- **What You Need to Know:** Study vulnerabilities and security mitigation strategies for mobile networks.

Learning Activities

u02s1 - Activity Overviews

Assignment Overview

In the assignment for this week, you will create a PowerPoint presentation that describes identified threats to a mobile network, discusses the impact to businesses and to the mobile network operator of these threats, and recommendations for mitigating these threats.

u02s2 - What You Need to Know

Threats and Vulnerabilities Found in Mobile Networks

The following resources provide information about the threats and vulnerabilities found in mobile networks.

- Bhasker, D. (2016). 4G LTE security for mobile network operators. *Journal of Cybersecurity and Information Systems 1*(4). Retrieved from https://www.csiac.org/journal-article/4g-lte-security-for-mobile-network-operators/7/
    - This reading will help you understand the wide range of security vulnerabilities that exist in a 4G LTE environment.
- GSMA.com. (2019). *Mobile telecommunications security threat landscape* [PDF]. Retrieved from https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf
    - This reading adds further insight into mobile telecom security threats in general.

u02a1 - 4G LTE Security for Mobile Network Operators

Overview

In this assignment you will create an 8–10-slide PowerPoint presentation that provides recommendations to leadership. Include graphics and color to communicate key points and highlights for your recommendations.

Instructions

You are a cybersecurity consultant who specializes in mobile and wireless security. You have been asked by a large mobile network operator (MN0) (like AT&T or Verizon) to give a presentation to leadership that explains the current threat landscape for the Mobile Telecommunications Industry. Rely on your readings and Internet research to select what you believe to be the top three threats and prepare a presentation that describes the threat, discusses the impact on businesses and the mobile network operator of these threats, and provide recommendations for mitigating these threats. At the end of your presentation, discuss future trends in this industry and potential new threats that might emerge.

Submit your presentation by 11:59 pm Sunday of this week.

Additional Requirements

- **Presentation**: Ensure the presentation is free of errors that detract from the overall message. Be sure to include graphics and color as part of your presentation.
- **Length of presentation**: Submit 8–10 presentation slides, a title slide, and a reference slide.
- **Font and font-size**: Use appropriate font sizes for the readability of a PowerPoint presentation.
- **Sources**: Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
  - Identify the top three security threats to mobile networks.
  - Explain how each of the identified top three security threats can impact businesses and mobile network operators.
- **Competency 2: Compare and contrast different approaches to digital communication.**
  - Speculate about future trends in the mobile network industry and potential new threats that might emerge.
- **Competency 3: Analyze how mobile systems operate to facilitate secure data access and voice.**
  - Explain why each of the identified top three security threats present risk to a mobile network.
  - Provide recommendations for mitigating the identified top three security threats.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Create a persuasive argument advocating for a viewpoint or recommendation.
  - Integrate visual elements that clarify or highlight key points.

Introduction

The Need to Protect Mobile Devices in a BYOD World

With the advent of Bring Your Own Device (BYOD), it is critical that you are thorough in having your personal mobile device secured properly. This is important even if you do not work in a BYOD environment to ensure that your mobile device is secure and has the level of privacy that is optimal. In today's world, personal cybersecurity is one of the weak links.

We all need to do our part to practice strong personal cybersecurity techniques, for example, installing and implementing a VPN on your mobile phone, adding virus and malware protection, and adding two-factor authentication to the device. Encouraging others to do the same will help protect data in a world where Bring Your Own Device (BYOD) has become commonplace.

To-Do List

- **Discussion:** Participate in a discussion to complete hands-on work to ensure you are doing your part to practice strong personal cybersecurity techniques by installing and implementing a VPN on your mobile phone, add virus and malware protection, and add two-factor authentication to the device.
- **What You Need to Know:** Study how to secure and set up privacy for your mobile device.

Learning Activities

u03s1 - Activity Overviews

Discussion Overview

In the discussion for this week, you will complete hands-on work to ensure you are doing your part to practice strong personal cybersecurity techniques by installing and implementing a VPN on your mobile phone, add virus and malware protection, and add two-factor authentication to the device.

u03s2 - What You Need to Know

Securing and Setting Up Privacy

The following Internet readings will help guide you through securing and setting up privacy for your mobile device:

- Gul, M. (2019). How to configure your IPhone for internet privacy and security. Retrieved from https://www.ilounge.com/articles/how-to-configure-your-iphone-for-internet-privacy-and-security
- Android.com. Secure an Android device. Retrieved from https://source.android.com/security
- Apple.com. You have control over what you share. Retrieved from https://www.apple.com/privacy/control/
- Top10VPN.com. (2020). Top 10 best VPN services for USA. Retrieved from https://www.top10vpn.com/best-vpn-for-usa/?v=control&bsid=c33se1kw421&gclid=CjwKCAiA0svwBRBhEiwAHqKjFj6ltMcpQj7XRtewytJFj8B-nL5uDkeNE9FLRMFpnNF8osRg2xl-qhoCUaUQAvD_BwE

u03d1 - Write Your Discussion Post

Hands-on Personal Mobile Device Security and Privacy

With the advent of Bring Your Own Device (BYOD), it is critical that you are thorough in having your personal mobile device secured properly. This is important even if you do not work in a BYOD environment to ensure that your mobile device is secure and has the level of privacy that is optimal. In today's world, personal cybersecurity is one of the weak links. The hands-on work you perform for this discussion topic will ensure you are doing your part to practice strong personal cybersecurity techniques. In this discussion topic, you will first follow instructions from your online reading to install and implement a VPN on your mobile phone, add virus and malware protection, and add two-factor authentication to the device. You will also set up facial recognition or fingerprint id.

Once you have completed the hands-on exercise, write a 3 to 4 paragraph response describing how you completed these tasks for your particular type of device. Discuss the mobile VPN you chose to use and explain why this was your choice. Discuss the level of difficulty or ease of installing and implementing the VPN. Finally, at the end of your response, write a persuasive email that you might send to family and friends encouraging them to take similar steps to secure their device security and privacy. Explain the importance of securing these devices appropriately and be sure you are speaking in layman's language.

Response Guidelines

In your response, use at least one of the assigned readings or audiovisual resources to support your points.

Read the posts of your peers and respond to two of them. How do your peers' opinions and results contrast with your own? Do you agree or disagree with the analysis of your peers? Explain.

Course Resources

Graduate Discussion Participation Scoring Guide

Unit 4 >> Bring Your Own Device – Security Implications

Introduction

Implications of BYOD Security

Employees and executives are used to relying on their personal mobile devices for fast access to important information. Because of this, employees and leaders at work organizations want the convenience of using a single device for work and personal use. As can be expected, many security issues arise with the implementation of Bring Your Own Device (BYOD) in the workplace. The security issues exist for both employees' personal data and the organization's business data and access. For employees, the added strain of being always connected and always available for organizational work can create a high level of stress not only for the employee but for the employee's family as well. Also, personal data stored on an employee's mobile device can be at risk. For example, if an employee's personal mobile device is lost or stolen, the company can auto-erase all data on the device. This can be a devastating loss of photos, music, and other personal documents if the appropriate backup is not in place. There will likely also be restrictions on what activities the device owner can perform on their own devices.

For the organization, BYOD provides a cost-effective means of increasing employee productivity. The use of BYOD usually improves employee morale as well. The issues that arise for the organization is in trying to maintain and manage the security needs for a wide variety of personal device products. When implementing BYOD there is an increased security risk for business assets. Many security controls need to be implemented when implementing BYOD. Additional employee training will also be necessary to ensure that all employees understand how to secure their devices and the importance of doing so. Employees also need to be trained on appropriate mobile device

behaviors to ensure the safety of their own data and the organization's data.

To-Do List

- **Assignment:** Write a report that evaluates the use of Bring Your Own Device (BYOD) in an organization and provides a recommendation to leadership either for or against the use of BYOD.
- **What You Need to Know:** Study how Bring Your Own Device (BYOD) is perceived by both employees and leadership and highlight the issues and benefits of installing and implementing BYOD in an organization.

Learning Activities

u04s1 - Activity Overviews

Assignment Overview

In the assignment for this week, you will write a report that evaluates the use of Bring Your Own Device (BYOD) in an organization and provides a recommendation to leadership either for or against the use of BYOD.

u04s2 - What You Need to Know

Bring Your Own Device (BYOD)

The readings below will provide insights into how Bring Your Own Device (BYOD) is perceived by both employees and leadership. They also highlight the issues and benefits of installing and implementing BYOD in an organization.

- Baillette, P., Barlette, Y., & Leeclercq-Vandelannoitte, A. (2018). Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end-users. *International Journal of Information Management, 43*, 76–84.
- Gökçe, K. G., & Doerlioglu, O. (2019). "Bring your own device" policies: Perspective of both employees and organizations. *Knowledge Management & E-Learning, 11*(2), 233–246.

u04a1 - Bring Your Own Device: Security Implications

Overview

In this assignment, you will write a 5–6 page report that evaluates the use of Bring Your Own Device (BYOD) in an organization and provides a recommendation to leadership either for or against the use of BYOD. You will support your evaluation and recommendation through the analysis of research you conduct using the internet.

Instructions

You are the CIO of a large financial organization. The CEO has talked with you about the operational benefits of implementing BYOD as well as the positive attitudes employees have about this possibility. You understand the security threats that BYOD can introduce to the organization and you have briefly discussed this with the CEO. He has now asked you to prepare a thorough report that evaluates the risks of BYOD implementation, potential threats with both of these weighed against the benefits. Use the information from your readings and research you perform on the Internet to provide this detailed analysis. At the end of your report, make a well-justified recommendation for or against implementing BYOD and be sure your recommendation is supported by your research and reading. Cite all relevant sources and provide a reference list using APA format.

Your detailed report should include the following:

- Benefits to employees.
- Risks to employees.
- Benefits to the organization and specifically for a financial organization.
- Risks to the organization and specifically for a financial organization.
- Potential specific threats with at least one example of each threat type that has already occurred in another organization.
- Recommended controls to prevent these threats.
- Your final recommendation with full justification.

Submit your report by 11:59 Sunday of this week.

Additional Requirements

- **Written communication:** Ensure written communication is free of errors that detract from the overall message.
- **Length of paper:** Submit 5–6 typed, double-spaced report pages, a title, and a reference page.
- **Format:** Format resources and citations according to APA guidelines for style and format.
- **Font and font-size:** Use Times New Roman 12-point font.
- **Sources:** Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
  - Summarize the benefits and risks of Bring Your Own Device (BYOD) environment to employees of a financial organization.
  - Summarize the benefits and risks of a Bring Your Own Device (BYOD) environment to a financial organization.
- **Competency 3: Analyze how mobile systems operate to facilitate secure data access and voice.**
  - Evaluate the risks of Bring Your Own Device (BYOD) implementation in a financial organization.
  - Provide a recommendation either for or against the use of Bring Your Own Device (BYOD) in a financial organization based upon analysis of your inter research.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Support main points, assertions, arguments, conclusions, or recommendations with relevant and credible evidence.
  - Use paraphrasing and summarization to represent ideas from external sources.

Unit 5 >> Smartphone and IoT Security

Introduction

The Need to Protect Devices and Networks in an IoT World

In order to adequately protect mobile and Internet of Things (IoT) devices and networks, a broad range of knowledge is required. This week provides an overview of security threats that exist across smartphones and IoT devices. Typical threats and attacks include the following:

- Physical threats related to losing a device or having it stolen.
- Software threats related to applications, networks, and device operating systems.

Further detail in this area would include poorly secured wifi connections, poorly implemented authentication procedures, lack of

encrypted data, trojans and malware, inadequate permission settings, and unprotected ports.

You will read about phishing attacks, malware, and man in the middle attacks during this week.

To further your understanding of this complex and multi-layered topic, you will read about three case studies comparing issues in IOS and Android devices.

To-Do List

- **Prepare:** Create a lab report as directed in the Jones and Bartlett Lab to incorporate into the assignment for this week.
- **Assignment:** Complete a hands-on lab and write an essay about conducting scanning and enumeration on a target network.
- **What You Need to Know:** Study how to take action against security threats to smartphones and Internet of Things (IoT) devices.

Learning Activities

u05s1 - Activity Overviews

Assignment Overview

In the assignment for this week you will complete a hands-on lab and write an essay about performing passive reconnaissance on a target organization.

u05s2 - What You Need to Know

Security Threats to Smartphone and Internet of Things (IoT) Devices

The following resources will help you understand how to take action against security threats to smartphone and Internet of Things (IoT) devices.

- Adăscăliţei, I. (2019). Smartphones and IoT security. *Informatica Economica, 23*(2), 63–71.
- Yan, P., & Zheng, Y. (2018). A survey on dynamic mobile malware detection. *Software Quality Journal, 26*(3), 891–919.

- Verkijika, S. F. (2019). If you know what to do, you will take action to avoid mobile phishing attacks: Self-efficacy, anticipated regret, and gender *Computers in Human Behavior, 101*, 28–296.

u05v1 - Hands-on Lab: Ethical Hacking: Conducting Scanning and Enumeration on a Target Network

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities. Be prepared to describe the following lab activities in the assignment for this week.

1. Understand the benefits of and tactics for conducting scanning and enumeration.
2. Perform network and system scans and export the results.
3. Capture network traffic and investigate packet-level data.
4. Understand how to start and configure Metasploit and its supporting services.
5. Perform and customize vulnerability scans and interpret the results.

Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning..

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Lab report with screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

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

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

u05a1 - Lab: Conducting Scanning and Enumeration on a Target Network

Overview

In this assignment, you will submit a 1–2-page essay that addresses the questions presented in this assignment and includes the lab report from the lab for this week. You must complete the lab before completing this assignment.

Instructions

In your essay for this assignment describe the following activities you completed for the Conducting Scanning and Enumeration on a Target Network lab.

1. Understand the benefits of and tactics for conducting scanning and enumeration.
2. Perform network and system scans and export the results.
3. Capture network traffic and investigate packet-level data.
4. Understand how to start and configure Metasploit and its supporting services.
5. Perform and customize vulnerability scans and interpret the results.

In your own words, describe what you learned from this lab on conducting scanning and enumeration on a target network.

Perform research on the Internet to understand security threats and attack vectors in a Bring Your Own Device (BYOD) scenario. How could scanning and enumeration be done in this type of environment? What security controls would you recommend implementing to avoid this type of scanning and enumeration?

Submit your essay including the lab report for this assignment by 11:59 pm on Sunday of this week.

Additional Requirements

- **Written communication:** Ensure written communication is free of errors that detract from the overall message.
- **Length of paper:** 1–2 typed, double-spaced essay pages, lab report pages, title page, and a reference page.
- **Format:** Format resources and citations according to APA guidelines for style and format.
- **Font and font-size:** Use Times New Roman 12-point font.
- **Sources:** Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
    - Apply internet research findings to analyze core concepts and applied technologies regarding security threats and attack vectors in a Bring Your Own Device (BYOD) context.

- **Competency 3: Analyze how mobile systems operate to facilitate secure data access and voice.**
  - Describe scanning and enumeration on a target network in a lab context.
  - Recommend security controls to implement to avoid scanning and enumeration in a Bring Your Own Device (BYOD) context.
- **Competency 4: Apply network defense tools to identify and mitigate mobile network security concerns.**
  - Complete the lab tasks as described in the lab learning objectives.
  - Describe how scanning and enumeration can be applied in a Bring Your Own Device (BYOD) context.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Organize content so ideas flow logically with smooth transitions.
  - Convey clear meaning through appropriate word choice and usage.

Unit 6 >> IoT Network Security in Healthcare Environment

Introduction

The Need for IoT Security in Healthcare Settings

One of the areas of greatest risk in the use of the Internet of Things (IoT) devices is in healthcare settings. Personally identifiable healthcare information is very valuable to hackers and although IoT provides excellent benefits for improved healthcare, the dangers of exposing patient data to nefarious actors have also increased.

Healthcare settings commonly use wearable patient recording devices that send data back to hospitals, labs, and physicians which make this data vulnerable to threats. Identification of security vulnerabilities and potential security controls that could be introduced in a healthcare environment is critical for the protection of data communication in an IoT world.

To-Do List

- **Assignment:** Write an essay that evaluates the use of the Internet of Things (IoT) devices in healthcare settings and provides potential mitigation to reduce security threats due to the use of IoT devices.
- **What you Need to Know:** Study elements and characteristics specific to Internet of Things (IoT) devices used in healthcare settings.

Learning Activities

u06s1 - Activity Overviews

Assignment Overview

In the assignment for this week you will write an essay that evaluates the use of the Internet of Things (IoT) devices in healthcare settings and provides potential mitigation to reduce security threats due to the use of IoT devices.

u06s2 - What You Need to Know

Internet of Things (IoT) Security Risks in Healthcare Settings

The following resources provide information about Internet of Things (IoT) security risks in healthcare settings:

- Burhan, M., Rehman, R. A., Khan, B., & Byung-Seo, K. (2018). IoT Elements, layered architectures, and security issues: A comprehensive survey. *Sensors, 18*(9).
- Onasanya, A., Lakkis, S., & Elshakankiri, M. (2019). Implementing IoT/WSN based smart Saskatchewan Healthcare System. *Wireless Networks, 25*(7), 3999–4020.
- Deebak, B. D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2019). An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. IEEE Access, 7, 135632–135649.

u06a1 - IoT Network Security in a Healthcare Environment

Overview

For this assignment you will write a 4–5-page essay that evaluates the use of the Internet of Things (IoT) devices in healthcare settings and provides potential mitigation to reduce security threats due to the use of IoT devices.

You will support your evaluation and potential mitigation based upon the study resources for this week.

Instructions

One of the areas of greatest risk in the use of the Internet of Things (IoT) devices in healthcare settings. Personally identifiable healthcare information is very valuable to hackers and although IoT provides excellent benefits for improved healthcare, the dangers of exposing patient data to nefarious actors has also increased.

In this assignment, you will explore the security vulnerabilities and potential security controls that could be introduced in a healthcare environment using wearable patient recording devices that send data back to hospitals, labs, and physicians. For the assignment, select one of three scenarios:

- A private physician's practice that receives patient data transmitted from the patient's device while at home.
- A lab environment that receives and analyzes patient data from either a patient in his or her home or in a hospital setting.
- A hospital where patient data is received at nursing stations from devices worn by patients in the hospital rooms.

Discuss security issues that are unique to the scenario you chose. Be sure to provide specific examples. Based on this week's reading, be sure to include a discussion of the following IoT elements and layers with regard to the security threats and potential security mitigation.

1. Identification
2. Sensing
3. Communication
4. Computation
5. Services
6. Semantics

Also, frame your discussion within the layers of the IoT architecture:

1. Perception Layer
2. Network Layer
3. Application Layer
4. Support Layer

Include a conclusion paragraph that summarizes the identified threats and related recommended mitigation.

Submit your essay for this assignment by 11:59 pm on Sunday of this week.

Additional Requirements

- **Written communication:** Ensure written communication is free of errors that detract from the overall message.
- **Length of paper:** 4–5 typed, double-spaced essay pages, title page, and reference page.

- **Format:** Format resources and citations according to APA guidelines for style and format.
- **Font and font-size:** Use Times New Roman 12-point font.
- **Sources:** Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
  - Explain security threats and potential security mitigation in the context of IoT elements and layers.
  - Use the layers of the IoT architecture to frame an analysis of security issues in healthcare settings due to the use of Internet of Things (IoT) devices.
- **Competency 2: Compare and contrast different approaches to digital communication.**
  - Identify security issues that are unique to a given healthcare setting due to the use of the Internet of Things (IoT) devices.
  - Summarize identified threats and related recommended mitigation unique to a given healthcare setting due to the use of the Internet of Things (IoT) devices.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Support main points, assertions, arguments, conclusions, or recommendations with relevant and credible evidence.
  - Use paraphrasing and summarization to represent ideas from external sources.

Unit 7 >> Secure Wireless LAN Implementation

Introduction

The Need for WLAN Security

Many organizations leverage the mobility and flexibility offered by wireless networks (WLAN). However, WLAN exposes organizations to risks not found in a wired network. Wireless access point devices are easy to acquire and easy to configure. An unauthorized wireless access device's connect to an access point in an organization's network could allow unauthorized users to access the network and, possibly, proprietary and confidential systems. Lack of encryption, sharing passwords, careless broadcasting of network names, or

SSID (Single System Identifiers) create inherent risks, threats, and vulnerabilities within WLAN infrastructures. It is critical to the security of data communication in a WLAN infrastructure to audit for potential vulnerabilities and weaknesses, and apply security countermeasures to mitigate security threats due to those vulnerabilities and weaknesses.

To-Do List

- **Prepare:** Create a lab report as directed in the Jones and Bartlett Lab to incorporate into the assignment for this week.
- **Assignment:** Complete a hands-on lab and write an essay about auditing a wireless network and planning for a secure WLAN implementation.
- **What You Need to Know:** Study how to implement a secure WLAN.

Learning Activities

u07s1 - Activity Overviews

Assignment Overview

In the assignment for this week, you will complete a hands-on lab and write an essay about auditing a wireless network and planning for a secure WLAN implementation.

u07s2 - What You Need to Know

Implementing and Securing a Wireless Network (WLAN)

The following resources provide information about implementing and securing a wireless network (WLAN):

- Fang, D. (2019). Efficient and flexible solutions for 5G wireless network security. Dissertation (ProQuest).
  - Skim through this dissertation.
- Kalniņš, R., Puriņš, J., & Alksnis, G. (2017). Security evaluation of wireless network access points. *Applied Computer Systems, 21*(1), 38–45.
- Lachance, D. (2015). *Systems security certified practitioner: Wireless transmission security.* [Video] Skillsoft Ireland.
- Moran, J. (n.d.) *CompTIA Security+ SY0-501: Wireless security settings* [COURSE]. Skillsoft.

u07v1 - Hands-on Lab: Hacker Techniques, Tools, and Incident Handling (3rd Edition): Auditing a Wireless Network and Planning for a Secure WLAN Implementation

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities. Be prepared to describe the following lab activities in the assignment for this week.

1. Review WLAN protocol scans, and identify wireless access points that may be open or using a weak encryption standard.
2. Perform a security assessment on a WLAN implementation using WEP/WPA/WPA2 encryption implementations on a wireless access point.
3. Review Kali and the Aircrack-ng suite of tools to decrypt previously captured scans and captures of WLAN traffic and WLAN encryption.
4. Mitigate weaknesses and security threats commonly found in WLAN implementations with proper security countermeasures.
5. Create a WLAN security implementation plan to address the confidentiality, integrity, and availability of WLAN services.

Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Lab report with screen captures from the lab.
- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

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

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

u07a1 - Lab: Auditing a Wireless Network and Planning for a Secure WLAN Implementation

Overview

In this assignment, you will submit a 1–2-page essay that addresses the questions presented in this assignment and includes the lab report from the virtual lab for this week. You must complete the lab before completing this assignment.

Instructions

In your essay for this assignment describe the following activities you completed for the Auditing a Wireless Network and Planning for a Secure WLAN Implementation lab.

1. Review WLAN protocol scans, and identify wireless access points that may be open or using a weak encryption standard.
2. Perform a security assessment on a WLAN implementation using WEP/WPA/WPA2 encryption implementations on a wireless access point.
3. Review Kali and the Aircrack-ng suite of tools to decrypt previously captured scans and captures of WLAN traffic and WLAN encryption.
4. Mitigate weaknesses and security threats commonly found in WLAN implementations with proper security countermeasures.
5. Create a WLAN security implementation plan to address confidentiality, integrity, and availability of WLAN services.

In your own words, describe what you learned from this lab on auditing a wireless network and planning for a secure wireless LAN implementation.

Perform research on the Internet to understand security threats and attack vectors in a wireless network scenario. What do you identify as the key elements in implementing a secure wireless LAN? What security controls would you recommend implementing to ensure a secure wireless LAN?

Submit your essay including the lab report for this assignment by 11:59 pm on Sunday of this week.

Additional Requirements

- **Written communication:** Ensure written communication is free of errors that detract from the overall message.
- **Length of paper:** 1–2 typed, double-spaced essay pages, lab report pages, title page, and reference page.
- **Format**: Format resources and citations according to APA guidelines for style and format.
- **Font and font-size:** Use Times New Roman 12-point font.
- **Sources:** Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
  - Identify the key elements in implementing a secure wireless LAN.
  - Apply your internet research findings to analyze core concepts and applied technologies regarding security threats and attack vectors in a WLAN context.
- **Competency 2: Compare and contrast different approaches to digital communication.**
  - Recommend security controls to implement to ensure a secure wireless LAN.
- **Competency 5: Apply network defense tools to identify and mitigate wireless security concerns.**
  - Complete the lab tasks as described in the lab learning objectives.
  - Describe auditing a wireless network and planning for a secure wireless LAN implementation in a lab context.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Organize content so ideas flow logically with smooth transitions.
  - Convey clear meaning through appropriate word choice and usage.

Unit 8 >> Wireless Sensor Networks

Introduction

The Need for Security in Wireless Sensor Networks

Wireless Sensor Networks found in systems used for monitoring and detection, for example, forest fire detection or traffic monitoring, present their own set of data communication vulnerabilities and mitigation strategies. This is due to the characteristics specific to Wireless Sensor Networks like the use of sensor nodes, and the physical security of the nodes in an environment that can be harsh. Understanding these characteristics and the elements of a Wireless Sensor Networks is essential for determining possible mitigation strategies.

To-Do List

- **Assignment:** Write an essay that evaluates potential vulnerabilities of a Wireless Sensor Network and provides possible mitigation strategies to address vulnerabilities of a Wireless Sensor Network.
- **What You Need to Know:** Study network and software architecture of Wireless Sensor Networks. You will also review operating systems related to the Internet of Things that are used in Wireless Sensor Networks.

Learning Activities

u08s1 - Activity Overviews

Assignment Overview

In the assignment for this week you will write an essay that that evaluates potential vulnerabilities of a Wireless Sensor Network and provides possible mitigation strategies to address vulnerabilities of a Wireless Sensor Network.

u08s2 - What You Need to Know

Network and Software Architecture of Wireless Sensor Networks

The following resources will help you understand network and software architecture of Wireless Sensor Networks, and review operating systems related to the Internet of Things that are used in Wireless Sensor Networks.

- Welton, T. (2015). *Internet of things: Introduction to IoT operating systems* [Video]. Skillsoft Ireland Limited.
- Welton, T. (2015). *Internet of things: Additional IoT operating systems* [Video]. Skillsoft Ireland Limited.
- Vijayalakshmi, S. R., & Muruganand, S. (2018). *Wireless sensor networks: An introduction*. Mercury Learning.
    - Chapter 1: Wireless Sensor Networks
    - Chapter 2: Node Hardware Architecture
    - Chapter 3: Software Architecture
    - Appendix A: A Guide to Securing Networks for WI-FI (IEEE 802.11 Family)

u08a1 - Wireless Sensor Networks: Threats and Mitigation

Overview

For this assignment, you will write a 4–5-page essay that evaluates potential vulnerabilities of a Wireless Sensor Network and provides possible mitigation strategies to address vulnerabilities of a Wireless Sensor Network. You will support your evaluation and potential mitigation based upon the study resources for this week.

Instructions

Select from the following wireless sensor network scenarios each of which is relevant to current events occurring in today's world:

- Forest Fire Detection - Sensor nodes detect smoke and temperature to indicate a fire has started. Sensors measure heat, humidity, and gas production.
- Water Quality Detection - Sensor nodes provide information on water quality and attributes in the ocean, rivers, lakes, water reserves, and dams. This wide range of monitoring can help detect poor water quality and where it is originating.
- Enemy Intrusion Monitoring for the Military - Sensor nodes provide information on enemy movement and intrusion into specific areas.
- Traffic monitoring - Sensor nodes provide information on traffic volume and traffic patterns, accidents, speed of traffic, and other roadside incidents that could pose a danger to drivers.

In your paper, consider the following elements of a Wireless Sensor Network as you discuss the vulnerabilities and possible mitigation strategies for your scenario:

1. Sensor nodes use batteries that provide constraints.
2. How are node failures detected and handled?
3. Sensor nodes often exist in harsh environmental conditions.
4. The physical security of the unattended nodes presents a vulnerability.
5. How is data securely transmitted to servers?
6. How can data encryption be handled in this low power environment?

Include a conclusion paragraph that summarizes the vulnerabilities and possible mitigation strategies for a Wireless Sensor Network.

Submit your essay for this assignment by 11:59 pm on Sunday of this week.

Additional Requirements

- **Written communication:** Ensure written communication is free of errors that detract from the overall message.
- **Length of paper:** 4–5 typed, double-spaced essay pages, title page, and reference page.
- **Format:** Format resources and citations according to APA guidelines for style and format.
- **Font and font-size:** Use Times New Roman 12-point font.

- **Sources:** Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
  - Analyze vulnerabilities and possible mitigation strategies in the context of the elements of a Wireless Sensor Network.
- **Competency 2: Compare and contrast different approaches to digital communication.**
  - Identify potential vulnerabilities of a Wireless Sensor Network that are unique to a given setting.
  - Summarize the vulnerabilities and possible mitigation strategies for a Wireless Sensor Network.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Support main points, assertions, arguments, conclusions, or recommendations with relevant and credible evidence.
  - Use paraphrasing and summarization to represent ideas from external sources.

Unit 9 >> Wireless Network Threat Landscape

Introduction

The Need to Protect a Network after it Has Been Compromised

Once a hacker has compromised a network it is critical to data communication on that network to monitor for post-exploitation, evasive maneuvers a hacker can use to hide their presence and avoid detection. Hacker's do this so they can conduct malicious activities such as extracting or modifying data, deploying malware, or extending their access deeper into the network. One way to monitor for this type of malicious activity is through Egress Filtering. Egress Filtering is used to prevent an outbound network from leaving the protected network.

To-Do List

- **Discussion:** Participate in a discussion to provide a mitigation strategy that you will apply in your home wireless network to mitigate identified risks.
- **Prepare:** Create a lab report as directed in the Jones and Bartlett Lab to incorporate into the assignment for this week.
- **Assignment:** Complete a hands-on lab and write an essay about performing post-exploitation activities and evasive maneuvers.
- **What You Need to Know**: Study the threat landscape related to wireless networks.

Learning Activities

u09s1 - Activity Overviews

Discussion Overview

In the discussion for this week, you will provide a mitigation strategy that you will apply in your home wireless network to mitigate identified risks.

Assignment Overview

In the assignment for this week you will complete a hands-on lab and write an essay about performing post-exploitation activities and evasive maneuvers.

u09s2 - What You Need to Know

Wireless Network Threat Landscape

The following readings, videos, and course will introduce you to the threat landscape related to wireless networks:

- U.S. Department of Homeland Security: CISA. (2019). Security tip (ST05-003) - Securing wireless networks. Retrieved from https://www.us-cert.gov
- Shannon, M. (2016). *CISA: Wireless security threats and mitigation* [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). *Certified ethical hacker - CEHv10: Wireless hacking common threats.* [Course]. Skillsoft Ireland Limited.

u09d1 - Write Your Discussion Post

Risks to Your Home Wireless Network

Select two potential risks to your home wireless network (either from this week's assigned reading or through your own Internet research). Describe the two risks in detail. Provide a mitigation strategy that you will apply in your home wireless network to mitigate these two risks. Be sure to cite at least two sources in your response.

Response Guidelines

Provide a response to at least two other students, analyzing their proposed mitigation strategy and stating whether you agree or disagree with the strategy and why.

Course Resources
Graduate Discussion Participation Scoring Guide

u09v1 - Hands-On Lab: Ethical Hacking: Performing Post-exploitation Activities and Evasive Maneuvers

Lab Activity – Jones & Bartlett Learning

Read the requirements for all related course activities before completing this lab. Take notes as needed as you complete the lab to help you complete those activities. Be prepared to describe the following lab activities in the assignment for this week.

1. Use a port scanner to verify egress filtering.
2. Confirm egress filtering by scripting reverse shell connections.
3. Obfuscate shell code to thwart antivirus scanning.
4. Package malware to be delivered through a web browser.

Select the linked title heading above to access a lab arranged through Jones & Bartlett Learning.

Follow the lab instructions carefully, making sure to perform all screen captures as instructed.

To demonstrate your understanding of core concepts and procedures used in the lab, you may be required to submit the following as part of the related activity:

- Lab report with screen captures from the lab.

- Other completed documentation as appropriate.

Jones & Bartlett Technical Support

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

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

u09a1 - Lab: Ethical Hacking: Performing Post-exploitation Activities and Evasive Maneuvers

Overview

In this assignment you will submit a 1- 2 page essay that addresses the questions presented in this assignment and includes the lab report from the virtual lab for this week. You must complete the lab before completing this assignment.

Instructions

In your essay for this assignment describe the following activities you completed for the Performing Post-Exploitation Activities and Evasive Maneuvers lab.

1. Use a port scanner to verify egress filtering
2. Confirm egress filtering by scripting reverse shell connections
3. Obfuscate shell code to thwart antivirus scanning
4. Package malware to be delivered through a web browser

In your own words, describe what you learned from this lab on performing post-exploitation activities and evasive maneuvers.

Perform research on the Internet to understand security threats and attack vectors in a wireless network scenario. How could post-exploitation activities and evasive maneuvers be done in this type of environment? What security controls would you recommend implementing to avoid these post-exploitation activities and evasive maneuvers from being effective?

Submit your essay including the lab report for this assignment by 11:59 pm on Sunday of this week.

Additional Requirements

- **Written communication:** Ensure written communication is free of errors that detract from the overall message.

- **Length of paper:** 1-2 typed, double-spaced essay pages, lab report pages, title page, and reference page.
- **Format**: Format resources and citations according to APA guidelines for style and format.
- **Font and font-size:** Use Times New Roman 12-point font.
- **Sources:** Cite at least two sources.

Competencies Measured

By successfully completing this assignment, you will demonstrate your proficiency in the following course competencies and assignment criteria.

- **Competency 1: Describe the core concepts, technologies, components, and security issues related to mobile and wireless networks.**
  - Apply internet research findings to analyze core concepts and applied technologies regarding security threats and attack vectors in a network context.
- **Competency 2: Compare and contrast different approaches to digital communication.**
  - Describe performing post-exploitation activities and evasive maneuvers to avoid detection in a network in a lab context.
  - Recommend security controls to implement to prevent post-exploitation activities and evasive maneuvers to avoid detection in a network context.
- **Competency 5: Apply network defense tools to identify and mitigate wireless security concerns.**
  - Complete the lab tasks as described in the lab learning objectives.
  - Describe how performing post-exploitation activities and evasive maneuvers to avoid detection can be applied in a network context.
- **Competency 6: Exhibit proficiency in writing, critical thinking, and research topic areas in real-life data communication networks.**
  - Organize content so ideas flow logically with smooth transitions.
  - Convey clear meaning through appropriate word choice and usage.

Unit 10 >> Identification and Tracking Technologies (RFID)

Introduction

The Need for Security in an RFID World

RFID (Radio Frequency Identification) is commonly used in warehouses and manufacturing to control inventory management. RFID systems present their own set of data communication

vulnerabilities and mitigation strategies. Understanding these characteristics of an RFID system is essential for determining possible mitigation strategies for potential vulnerabilities and threats specific to an RFID system.

To-Do List

- **Discussion:** Participate in a discussion to create a PowerPoint presentation that describes the benefits of implementing this type of RFID technology but to also highlight any serious security issues that will arise due to the use of RFID to manage the inventory and warehouse.
- **What You Need to Know:** Study a comprehensive overview of Bluetooth and RFID security concepts, and you will review a case study of RFID implementation and effectiveness to improve a food-related supply chain.

Learning Activities

u10s1 - Activity Overviews

Discussion Overview

In the discussion for this week, you will create a PowerPoint presentation that describes the benefits of implementing RFID technology for improved inventory and warehouse management and highlights any serious security issues that will arise due to the use of RFID to manage the inventory and warehouse.

u10s2 - What You Need to Know

Bluetooth and RFID Security Concepts

The following readings will help you will gain a comprehensive overview of Bluetooth and RFID security concepts and you will review a case study of RFID implementation and effectiveness to improve a food-related supply chain:

- Lorenzo, S. F., Benito, J. A., Cardarelli, P. G., Garaia, J. A., & Juaristi, S. A. (2019). A comprehensive review of RFID and Bluetooth security: Practical analysis. *Technologies, 7*(1), 15.
- Biswal, A. K., Jenamani, M., & Kumar, S. K. (2018). Warehouse efficiency improvement using RFID in a humanitarian supply chain: Implications for Indian food security system. *Transportation Research Part E: Logistics and Transportation Review, 109*, 205–224.

- Mansuri, S. (2019). Complete guide on RFID and its applications in supply chain management and logistics. Retrieved from https://www.peerbits.com/blog/rfid-applications-in-supply-chain-management-and-logistics.html

u10d1 - Write Your Discussion Post

Analyzing security of RFID implementation for Warehouse and Inventory Management

Assume you are a cybersecurity consultant and are working for a large warehouse management service that wants to implement RFID for improved inventory and warehouse management. You have been asked to provide a presentation that describes the benefits of implementing this type of RFID technology but to also highlight any serious security issues that will arise due to the use of RFID to manage the inventory and warehouse. Based on this week's reading and your own research on the Internet, create a 10–12 PowerPoint slide presentation for presentation to the organization's executive leadership team. On the final slide, make a recommendation for how the company can effectively and safely move to the use of RFID technology.

Response Guidelines

Post your presentation to the discussion board and then comment on at least two classmate's presentations indicating your agreement with their ideas and any area of disagreement that you might have.

Course Resources
Graduate Discussion Participation Scoring Guide