Preview: IAS5200 : Network Architecture and Cyberoperations

Syllabus

Course Overview

In this course, you will study common security architectures for the protection of information systems and data. You will develop skills to identify potential vulnerabilities in architectures and design secure architectures. You will learn how to identify issues related to the design and implementation of operating system concepts, components, and interfaces, and design and implement significant architectural changes to an existing operating system. You will also examine the authorities, roles, and steps associated with cyberoperations and develop a working knowledge of the security issues associated with building complex systems from third-party components of unknown origin.

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 these activities, please contact DisabilityServices@Capella.edu to request accommodations.

Course Competencies **(Read Only)**

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

1. Analyze potential vulnerabilities within a specific network architecture.
2. Implement architectural changes to a network to enhance security.
3. Evaluate the goals and objectives of each phase of a well-organized cyberoperation.
4. Explain the role of lifecycle management for continuous management of network security.
5. Analyze offensive and defensive cyberoperations.

6 Exhibit proficiency in writing, critical thinking, and researching topic areas in network architecture and cyberoperations.

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.). (2019). *IAS5200: Network architecture and cyberoperations* [Custom online lab bundle]. Burlington, MA: Jones & Bartlett.

Capella University (Ed.). (2019). *IAS5200: Network architecture and cyberoperations* [Custom text]. Burlington, MA: Jones & Bartlett.

Library

The following required resources 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.

- Axelrod, C. W. (2013). *Engineering safe and secure software systems.* Norwood, MA: Artech House.
- Behera, S. R. (2018). Chapter 18, Surface Web, deep Web, and dark net. In *Hacking exposed*, New Delhi, India: BPB Publications.
- Bigger, D. (2014). *CompTIA Network+ 2014: Vulnerability scanning and penetration testing* [Video]. Skillsoft Ireland.

- Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). Chapter 21, Protecting the perimeter. In *Cybersecurity essentials* (pp. 1–9). Skillsoft.
- Calder, A., & Watkins, S. (2012). *IT governance: An international guide to data security and ISO27001/ISO27002* (5th ed.). London, England: Kogan Page.
- CEHv10. (n.d.). *Hacking concepts* [Tutorial]. Skillsoft.
- CEHv10. (n.d.). *Wireless hacking common threats* [Tutorial]. Skillsoft.
- Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys, 51*(4), 1–36.
- Meyers, M. (2018). *CompTIA network+ certification all-in-one exam guide: Exam N10-007* (7th ed.). Columbus, OH: McGraw-Hill.
- Pipyros, K., Thraskias, C., Mitrou, L., & Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security,* 74, 371–383.
- Sampson, A. (2017). *CompTIA network+N10-007: Penetration testing* [Tutorial]. Skillsoft.
- Skillsoft. (n.d.). *IINS 3.0: Malware and data loss: Identify common malware types* [Tutorial].

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.

- Adams, M., & Reiss, M. (2018, Mar 4). International law and cyberspace: Evolving views [Blog post]. Retrieved from https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views
- Aftergood, S. (2018, Jul 17). Secrecy news: Cyber war as a career path [Blog post]. Retrieved from https://fas.org/blogs/secrecy/2018/07/cyber-war-training/
- Baram, G. (2018, Jun 19). The theft and reuse of advanced offensive cyber weapons pose a growing threat [Blog post]. Retrieved from https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat
- Bezsonoff, N. (2017, Aug 21). Your firewall won't save you from the next DDoS attack [Blog post]. Retrieved from https://www.itspmagazine.com/from-the-newsroom/your-firewall-wont-save-you-from-the-next-ddos-attack
- CFR Interactives. (2018). Cyber operations tracker. Retrieved from https://www.cfr.org/interactive/cyber-operations
- Cole, E. (2017). Offense must inform the defense – Is your cyber security program fixing the right problems. Retrieved from https://secure-anchor.com/offense-must-inform-defense/
- Curran, K. (2019). Firewalls. Retrieved from https://kevincurran.org/com320/labs/Firewall/securityfirewalls.html
- Ellis, D. (2015). A hacking scenario: How hackers choose their victims [Blog post]. Retrieved from https://www.securitymetrics.com/blog/hacking-scenario-how-hackers-choose-their-victims
- Gonzalez, K. (2018, Jun 8). A step-by-step guide to vulnerability assessment [Blog post]. Retrieved from https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/
- Goodman, R. (2018, Mar 8). Cyber operations and the U.S. definition of "armed attack" [Blog post]. Retrieved from https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/

- Henry, J. (2018, Aug 6). 7 ways to identify darknet cybersecurity risks [Blog post]. Retrieved from https://securityintelligence.com/7-ways-to-identify-darknet-cybersecurity-risks/
- Kilner, P. (2017, Dec 21). Ethics of cyber operations: '5th domain' creates challenges, needs new rules [Blog post]. Retrieved from https://www.ausa.org/articles/ethics-cyber-operations-%E2%80%985th-domain%E2%80%99-creates-challenges-needs-new-rules
- Multi-State Information Sharing and Analysis Center & United States Computer Emergency Readiness Team. (2005). *Malware threats and mitigation strategies* [White paper] [PDF]. Available from https://www.us-cert.gov/
- Netsparker. (2019). How to evaluate web application security scanners [Blog post]. Retrieved from https://www.netsparker.com/blog/web-security/how-to-evaluate-web-application-security-scanners-tools/
- Nibusinessinfo.co.uk. (2019). Website hosting options: Pros and cons of in-house hosting. Retrieved from https://www.nibusinessinfo.co.uk/content/pros-and-cons-house-hosting
- PentestTools. (2019). Website vulnerability scanner. Retrieved from https://pentest-tools.com/website-vulnerability-scanning/web-server-scanner
- Tech-FAQ. (2019). DMZ (DeMilitarized Zone). Retrieved from http://www.tech-faq.com/dmz.html
- United States Joint Chiefs of Staff. (2018). Joint publication 3-12: Cyberspace operations [PDF]. Available from https://www.jcs.mil/

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.

Library

The following optional Skillsoft resources are available via the Capella University Library.

- Skillsoft. (n.d.). *CISSP: Security engineering part 2* [Tutorial]. null

Unit 1 >> Life Cycle Management

Introduction

In Unit 1 we will introduce ICT life cycle management. The concepts of standards and application of frameworks will also be discussed. We will learn of the ISO 12207-2008 standard as well as how it can be tailored to fit the needs of a business.

Learning Activities

u01s1 - Studies

Readings

Use the Capella University Library to read the following:

- Axelrod, C. W. (2013). *Engineering safe and secure software systems*. Norwood, MA: Artech House.
  - Chapter 8, "Software System Development Processes," pages 157–176.
  - Appendix B, pages 253–256.
- Calder, A., & Watkins, S. (2012). *IT governance: An international guide to data security and ISO27001/ISO27002* (5th ed.). London, England: Kogan Page.
  - Chapter 7, "External Parties," pages 101–112.

Optional Skillsoft Resource

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *CISSP: Security engineering part 2* [Tutorial].

u01s1 - Learning Components

- Investigate formal agreement processes for ensuring security.
- Research the scope of ISO 12207-2008 in regard to network architecture.
- Describe life cycle management.
- Investigate options for offshore hardware and software development.

u01d1 - Security Implications of Offshoring Development

Offshoring hardware and software development introduces challenges to life cycle maintenance of products prone to vulnerabilities as well as response times to reports of those vulnerabilities. There have also been instances in which international politics influenced the product life cycle for imported products, such as when China grew suspicious that Microsoft was building back doors into their operating systems for NSA access in 2013–14. This seems prophetic in light of subsequent revelations.

Using the course materials and any research needed to fill in knowledge gaps, discuss the following:

- What are some ways that national and international politics can affect organizations that offshore the development of hardware and software products?
- How does offshoring of development impact the ability of organizations to respond quickly and effectively to vulnerabilities discovered in their products?
- What are your thoughts on the efficacy of U.S. companies offshoring development? Do you support this practice? Support your position with professional or scholarly evidence.

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide
Capella University Library

u01d1 - Learning Components

- Describe cyberoperations.
- Identify international laws that apply to cyberoperations.
- Describe life cycle management.
- Investigate options for offshore hardware and software development.

u01a1 - Life Cycle Management

Overview

For this assignment, discuss some of the tasks involved in ICT life cycle management and explain the steps in establishing a systematic ICT life cycle approach. Elaborate on the use of controls to ensure cooperation among relevant processes.

Instructions

Use the study materials and engage in any research needed to close knowledge gaps. Then, write a 2–3 page paper in which you:

- Explain the role of life cycle management in the production of secure ICT products.

- Describe the role and application of ISO 12207-2008 in shaping enterprise architecture.
- Explain the advantages of a formal agreement process in ensuring product quality and security.
- Explore the impact of outsourcing on life cycle management of secure ICT products.
- Explore the security implications of offshore development of software and hardware components.

Additional Requirements

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Format resources and citations according to current APA style and format.
- **Length of paper:** 2–3 pages of content plus title and references pages.
- **Font and font size:** Times New Roman, 12 point.

Course Resources
APA Style and Format
Capella University Library

u01s2 - Firewall Fundamentals

Your IAS5200 Network Architecture and Cyberoperations custom text was created for this course by Capella University in conjunction with Jones & Bartlett Learning to supply you with selected course materials from the following three textbooks:

- Harwood's 2016 *Internet Security: How to Defend Against Attackers on the Web*.
- Stewart's 2014 *Network Security, Firewalls, and VPNs*.
- Oriyano and Solomon's *2020 Hacker Techniques, Tools, and Incident Handling*.

In preparation for your work in Unit 2, use your *IAS5200: Network Architecture and Cyberoperations* custom text to read the following:

- Chapter 2, "Firewall Fundamentals," from Stewart's *Network Security, Firewalls, and VPNs*.

u01s2 - Learning Components

- Describe a firewall.
- Determine the steps in implementing a firewall.
- Describe usable firewall architectures.

Unit 2 >> Border Defenses

Introduction

In this unit, we will explore the design and architecture choices that make up a secure enterprise network border defense. The DMZ is used in most organizations and the design of the DMZ is similar in many situations. We will explore those commonalities in completing a secure DMZ and discuss ways that change management can be useful in reducing risk when the DMZ is compromised. In addition, we will explore the fundamentals of firewalls and how to implement a firewall most effectively.

Learning Activities

u02s1 - Studies

Readings

Use your *IAS5200: Network Architecture and Cyberoperations* custom text to read the following from Stewart's *Network Security*:

- Chapter 7, "Firewall Basics." Focus specifically on these sections:
  - "Firewall Rules."
  - "Authentication and Authorization."
  - "Monitoring and Logging."
  - "Understanding and Interpreting Firewall Logs and Alerts."
- Chapter 8, "Firewall Deployment Considerations."

Use the Internet to read the following:

- Nibusinessinfo.co.uk. (2019). Website hosting options: Pros and cons of in-house hosting. Retrieved from https://www.nibusinessinfo.co.uk/content/pros-and-cons-house-hosting
- Tech-FAQ. (2019). DMZ (DeMilitarized Zone). Retrieved from http://www.tech-faq.com/dmz.html

Optional Skillsoft Resources

Use the Capella library to complete the following:

- Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). Chapter 21, Protecting the perimeter. In *Cybersecurity essentials* (pp. 1–9). Skillsoft.
- Meyers, M. (2018). *CompTIA network+ certification all-in-one exam guide: Exam N10-007* (7th ed.). Columbus, OH: McGraw-Hill.

u02s1 - Learning Components

- Describe a firewall.
- Determine the steps in implementing a firewall.
- Describe usable firewall architectures.
- Explain how self-hosting a network exposes an organization to risk.
- Identify the purpose of the DMZ in a network.
- Compare the recommended uses for software and hardware firewalls.
- Explain the difference between a software and hardware firewall.
- Identify the pros and cons of outsourcing website hosting.
- Identify the pros and cons of self-hosting a website.

u02v1 - Lab: Configuring a pfSense Firewall on the Server

Read the requirements for all related course activities before completing this lab. Take notes throughout the lab to help you with those activities.

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

1. Follow the lab instructions carefully. Review the first two sections of this lab before moving on to the Lab Challenge and Analysis section of the lab.
2. Download and save the assignment template linked in Resources. For each lab in the course, you will populate a copy of the template with your lab screenshots and your assignment responses as indicated.
3. Take the following screenshots from Section 3:
    - Part 2: Make a screenshot of your Nessus scan configuration and scan results.
    - Part 3: Make a screenshot of the Command Prompt commands you use to add a persistent route.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template [DOCX]

u02v1 - Learning Components

- Determine the steps in implementing a firewall.

u02d1 - Implementing Firewalls

You are the senior security technician for a small retail business whose network does not have a firewall. You have been asked to evaluate the network and the overall security needs. You are debating the merits of using a single firewall versus two firewalls with a demilitarized zone (DMZ).

Examine the two diagrams in Network Diagrams (linked in Resources), then address the following:

1. If you use two firewalls, should they come from the same vendor? Explain your answer.
2. How would you explain the advantages you would expect to gain from the dual-firewall architecture?
3. What would be the downside of deploying a dual-firewall architecture?
4. Which servers would you place in the DMZ? Explain your answer.
5. If using the two-firewall architecture, what traffic would be allowed through each of the firewalls? Explain your response.
6. If one of the servers in the DMZ were a self-hosted web server, would this expose the organization to risk? Explain.

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide
Network Diagrams [DOCX]

u02d1 - Learning Components

- Describe a firewall.
- Determine the steps in implementing a firewall.
- Describe usable firewall architectures.
- Identify the purpose of the DMZ in a network.
- Compare the recommended uses for software and hardware firewalls.
- Explain the difference between a software and hardware firewall.

u02a1 - Firewalls and Website Hosting

Instructions

By now, you should have completed this unit's lab, Configuring a pfSense Firewall on the Server, and saved your screenshots into the assignment template.

Consider your lab work and studies to complete the following, clearly labeling each section.

1. Describe briefly what you learned and observed in the lab and include it in the section with your screenshots. Be specific in your description.
2. You are an IT security specialist for a startup retailer. The CIO has asked you to secure outbound connections from internal computers, protect internal resources from inbound Internet connections, and use a demilitarized zone (DMZ) segment to allow Internet connections to the organization's website, where customers place orders. The CIO asks you to do this with a single firewall. Consider the Unit 2 Assignment Diagram (linked in Resources) and indicate if you will place this single firewall at 1, 2, or 3. Explain your decision.
3. The CIO wants to self-host the company's website. As an IT security specialist, address the following questions:
    - What security risks does this pose for the organization?
    - Assuming a similar network design to that depicted on the diagram would be used, would you recommend hardware or software firewalls? Justify your choice.
    - Would there be advantages to outsourcing this website? If so, what would they be?
    - How would you write an informed recommendation to the CIO about whether you consider it better to self-host or outsource the website hosting? Justify your recommendation.

Additional Requirements

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **Font and font size:** Times New Roman, 12 point.

Refer to the scoring guide to ensure that you meet the grading criteria before submitting this assignment.

Course Resources

Unit 2 Assignment Diagram [DOCX]

Unit 3 >> Implementing Network Security

Introduction

Network security implementation is a complex process involving many elements. In this unit you will read about seven domains of an IT infrastructure, defense in depth (at every domain), protocols, addressing, system hardening, hardware selection, authentication, authorization, and accounting. Additional elements are encryption, hosts (remote, local, and mobile), redundancy, and endpoint security.

Learning Activities

u03s1 - Studies

Readings

Use your *IAS5200: Network Architecture and Cyberoperations* custom text to read the following from Stewart's *Network Security*:

- Chapter 5, "Network Security Implementation."

Skillsoft Resources

Use the Capella library to complete the following:

- Sampson, A. (2017). *CompTIA network+N10-007: Penetration testing* [Tutorial]. Skillsoft.

u03s1 - Learning Components

- Define firewall rule.
- Describe the elements of a firewall rule.
- Explain how firewall rules are added to a firewall.

u03d1 - Network Solution Scenario, Part 1

ABC Health Services Clinic needs your help in proposing a network solution to meet the clinic's requirements. The clinic's health care providers and lab technicians must be able to access patient charts, lab results, x-rays, and medication information from laptops while in the patients' rooms. The IT director of the clinic has purchased new servers that are housed in a data center in a secure area of the clinic on the first floor, where there are also patient rooms. These servers must always be accessible.

- One server houses the database of all patient records. All lab work, x-rays, and prescriptions are performed within the clinic and there is no need to exchange data with third parties outside of the clinic.

- The billing department invoices patients and accepts credit card payments. The billing department must also access the Internet to exchange data with insurance companies and Medicare. Thirty-five laptops are available for use by the health care providers on the clinic's wireless LAN (WLAN).
- Patient rooms are on three floors of the clinic. The health care providers must be able to access patient records via their laptops on all rooms on these floors. The IT director wants to ensure that strong network security exists as these changes are made.

For this discussion, analyze this scenario with regard to the seven domains of an IT infrastructure:

- What are the risks in each domain for this scenario?
- What security controls will be required for each domain for this scenario?

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide

u03d1 - Learning Components

- Define firewall rule.
- Identify potential strategies for preventing security breaches.
- Describe the elements of a firewall rule.
- Explain how firewall rules are added to a firewall.

u03d2 - Network Solution Scenario, Part 2

This discussion requires you to use the scenario presented in the first discussion in this unit:

> You are proposing a network solution for ABC Health Services Clinic. Patient charts, lab results, x-rays, and medication information must be accessible to medical staff from laptops while in the patients' rooms. There are new servers in a first-floor data center in a secure area of the clinic, where there are also patient rooms. These servers must be available at all times.
>
> - One server houses the database of all patient records. All lab work, x-rays, and prescriptions are performed within the clinic and there is no need to exchange data with third parties outside of the clinic.

- The billing department invoices patients and processes credit card payments. Billing must also access the Internet to exchange data with insurance companies and Medicare.

Thirty-five laptops are available for use by the health care providers on the clinic's wireless LAN (WLAN). Patient rooms are on three floors of the clinic. The health care providers must be able to access patient records via their laptops on all rooms on these floors. The IT director wants to maintain strong network security as these changes are made.

Complete the following:

- Discuss public and private addressing for this scenario.
- Discuss authentication, authorization, and accounting requirements for the health care providers accessing the network and retrieving patient health care information.
- Discuss communication encryption requirements.
- List questions would you ask the IT Director about the current redundancy of the system.

Response Guidelines

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

u03d2 - Learning Components

- Identify potential strategies for preventing security breaches.

u03s2 - Discussion Preparation

In preparation for a Unit 4 discussion, use the Internet to complete the following:

- Curran, K. (2019). Firewalls. Retrieved from https://kevincurran.org/com320/labs/Firewall/securityfirewalls.html
  - Download the Network Firewall Visualization Tool.

You will use the Network Firewall Visualization Tool to understand different firewall architectures and create firewall rules to protect against specific threats that you can define in the simulator. Refer to the Unit 4 Discussion Instructions [DOCX] to complete the discussion.

u03s2 - Learning Components

- Define firewall rule.

- Describe the elements of a firewall rule.
- Explain how firewall rules are added to a firewall.

Unit 4 >> Penetration Testing: Pen Testing a Firewall

Introduction

A *penetration test* is a simulation of a cyber attack that helps reveal vulnerabilities in a system. In this week's lab, you will perform a penetration test on a firewall. The results of your penetration test will inform the security policies and controls that you implement.

Learning Activities

u04s1 - Studies

Readings

Use your *IAS5200: Network Architecture and Cyberoperations* custom text to complete the following from Stewart's *Network Security*:

- Read Chapter 4, "Network Security Threats and Issues."
- Review Chapter 7, "Firewall Basics."

Skillsoft Resources

Use the Capella library to complete the following:

- Bigger, D. (2014). *CompTIA Network+ 2014: Vulnerability scanning and penetration testing* [Video]. Skillsoft Ireland.
- Sampson, A. (2017). *CompTIA network+N10-007: Penetration testing* [Tutorial]. Skillsoft.

u04s1 - Learning Components

- Define firewall rule.
- Describe penetration testing.
- Describe a vulnerability scan.
- Describe the elements of a firewall rule.
- Explain how firewall rules are added to a firewall.
- Compare and contrast vulnerability scans and penetration tests.

u04v1 - Lab: Penetration Testing a pfSense Firewall

Read the requirements for all related course activities before completing this lab. As you complete the lab, take notes to help you with these activities.

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

1. Follow the lab instructions carefully. Review Sections 1 and 2 before beginning Section 3. You will be discussing particular vulnerabilities identified in the scan, the ports affected, and recommended remediation. Section 3 is an unguided lab to provide situations similar to what would be encountered in the real world.
2. Take the following screenshots from Section 3:
    - Part 2:
        - The added ICMP Ping (-PE) option in the Quick Scan Profile of Zenmap.
        - The scan results after the above change was made.
    - Part 3:
        - The new firewall rules added to deny traffic from the TCP ports identified in the vulnerability report. Be sure the screenshot includes the rule and the description of what is being blocked.
3. Populate the assignment template (linked in Resources) with your lab screenshots and assignment responses.

Jones & Bartlett Technical Support

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

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

Course Resources
Assignment Template [DOCX]

u04v1 - Learning Components

- Describe penetration testing.

u04d1 - Risk Analysis, Vulnerability Testing, and Penetration Testing

You are a recently hired CIO for an Internet retailer. Prior to hiring you, upper management knew that they had to address security at a much more advanced level and were unclear about the differences among risk analysis, vulnerability testing, and penetration testing. As one of your first tasks, they would like you to prepare a report to help them understand the distinctions among the three and make recommendations to improve their system security. They are uncertain which of the three tests they should consider—or if all are essential, in which order they should be performed. It is your job to help them make sense of all this and provide a plan to improve the organization's cybersecurity. Your report may be a PowerPoint deck or a written response.

Response Guidelines

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

u04d1 - Learning Components

- Describe penetration testing.
- Describe a vulnerability scan.
- Compare and contrast vulnerability scans and penetration tests.

u04d2 - Firewall Rules

Follow the discussion instructions linked in Resources to use the Network Firewall Visualization Tool and address the following:

- Explain the rules that you created and your justification for those rules.
- If you could not create all the rules required to accomplish this, explain your efforts and thought process in evaluating the scenario and possible related firewall rules.
- List the questions you asked to determine which rules to create.

Response Guidelines

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

Course Resources

Graduate Discussion Participation Scoring Guide

Unit 4 Discussion Instructions [DOCX]

Firewalls

u04d2 - Learning Components

- Define firewall rule.
- Describe the elements of a firewall rule.
- Explain how firewall rules are added to a firewall.

u04a1 - Vulnerability Scans and Penetration Testing

By now, you should have completed the lab Penetration Testing a pfSense Firewall and saved your screenshots in the assignment template.

Instructions

Consider your lab work and studies as you add your responses to the following in the assignment template:

1. Describe briefly what you observed and learned in the lab and include it in the section with your screenshots. Be specific.
2. You are the lead security specialist for XYZ Corporation. They have recently experienced a significant breach and the CEO wants to ensure XYZ's systems and networks are secure. Your CIO has explained to you that due to budgetary constraints, you are limited to conducting a vulnerability assessment or a penetration test but not both. In 300–350 words, discuss the two options and provide your rationale for the choice that would be most likely to prevent another breach. Be sure to cite your sources.

Course Resources

APA Style and Format

Capella University Library

Unit 5 >> Internet Connection Risks

Introduction

Use of the Internet exposes individuals and businesses regularly to threats and risks that must be mitigated. Because the Internet is unregulated and not secure, it is the responsibility of those connecting to the Internet to mitigate risks such as malware, personal damage (such as identity theft, fraud, reputation damage), email attacks, and exposure to offensive content and predators. In this unit, you will learn about these attacks and best practices for mitigating the risks.

Learning Activities

u05s1 - Studies

Readings

Use your *IAS5200: Network Architecture and Cyberoperations* custom text to read the following from Harwood's *Internet Security: Howto Defend Against Attackers on the Web*:

- Chapter 4, "Mitigating Risk When Connecting to the Internet."

Use the Internet to read the following:

- Multi-State Information Sharing and Analysis Center & United States Computer Emergency Readiness Team. (2005). *Malware threats and mitigation strategies* [White paper] [PDF]. Available from https://www.us-cert.gov/

Skillsoft Resources

Use the Capella library to complete the following:

- Skillsoft. (n.d.). *IINS 3.0: Malware and data loss: Identify common malware types* [Tutorial].

u05s1 - Learning Components

- Identify vulnerabilities that exist in a Web application.
- Identify mitigation strategies for Web vulnerabilities.
- Identify vulnerabilities that exist in connection to the Internet.
- Describe what a vulnerability scan shows in its report.
- Identify vulnerabilities that exist on a website.
- Describe the process for interpreting a Web vulnerability scan.

u05d1 - Cyberattack Consultation Part 1

You are an IT security consultant called in to assist a small Web-based retailer where a cyberattack has occurred; customer data has been taken and the attacker is demanding payment. The business owner does not know how to proceed. Backups are only made once per week and it has been five days since the last backup. The company does not have an incident response plan or team—just a database administrator and a general IT technician. The IT tech reveals that he has not installed several necessary patches. Based on your readings and further research, what would you recommend to prevent a recurrence? In your response, consider the following:

- The seven domains of an IT infrastructure.
- Disaster recovery and business continuity.

Explain how you would advise the owner:

- What actions need to be taken and within what time period?
- What other decisions must be made?

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide

u05d1 - Learning Components

- Identify vulnerabilities that exist in a Web application.
- Identify tools that can be used to analyze Web servers, websites, and Web application tools.
- Identify mitigation strategies for Web vulnerabilities.
- Identify vulnerabilities that exist in connection to the Internet.
- Identify vulnerabilities that exist on a website.

u05d2 - Cyberattack Consultation Part 2

Continue in the scenario from the previous discussion.

As the IT security consultant hired to help a small Web-based retailer that was the victim of a recent cyberattack, you have been asked to educate the staff on best practices for connecting to the Internet. Provide an outline of the material you would include in this training. What unique aspects would need to be covered, based on the details of the scenario?

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide

u05d2 - Learning Components

- Identify vulnerabilities that exist in a Web application.
- Identify mitigation strategies for Web vulnerabilities.
- Identify vulnerabilities that exist in connection to the Internet.
- Identify vulnerabilities that exist on a website.

u05s2 - Unit 6 Preparation

The workload in Unit 6 is a bit heavier than in previous units. Consider taking some time this week for some of the assigned readings.

u05s2 - Learning Components

- Identify vulnerabilities that exist in a Web application.
- Identify tools that can be used to analyze Web servers, websites, and Web application tools.
- Identify vulnerabilities that exist in connection to the Internet.
- Identify vulnerabilities that exist on a website.

Unit 6 >> Vulnerability Scanning

Introduction

Previously, you learned about and performed a penetration test to expose vulnerabilities. This week you will perform a *vulnerability scan*, which inspects a system for possible points of an exploit and helps identify security vulnerabilities in the system. The vulnerability scan will also classify any detected weaknesses. The vulnerability scan can predict the effectiveness of certain security controls in mitigating the detected vulnerability. Vulnerability

scanning software analyzes details about the attack surface, comparing it to a database of known security issues in services and ports, packet anomalies, and exploitation paths for scripts and applications.

Learning Activities

u06s1 - Studies

Readings

Use your *IAS5200: Network Architecture and Cyberoperations* custom text to read the following from the Harwood text:

- Chapter 5, "Mitigating Website Risks, Threats, and Vulnerabilities."
- Chapter 7, "Securing Web Applications."

Use the Internet to complete the following:

- Gonzalez, K. (2018, Jun 8). A step-by-step guide to vulnerability assessment [Blog post]. Retrieved from https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/
- Netsparker. (2019). How to evaluate web application security scanners [Blog post]. Retrieved from https://www.netsparker.com/blog/web-security/how-to-evaluate-web-application-security-scanners-tools/
- PentestTools. (2019). Website vulnerability scanner. Retrieved from https://pentest-tools.com/website-vulnerability-scanning/web-server-scanner

u06s1 - Learning Components

- Identify vulnerabilities that exist in a Web application.
- Identify tools that can be used to analyze Web servers, websites, and Web application tools.
- Identify mitigation strategies for Web vulnerabilities.
- Identify vulnerabilities that exist in connection to the Internet.
- Describe what a vulnerability scan shows in its report.
- Identify vulnerabilities that exist on a website.
- Describe the process for interpreting a Web vulnerability scan.

u06v1 - Lab: Evaluating Web Server Vulnerabilities

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

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

1. Follow the lab instructions carefully. Before beginning, review Sections 1 and 2.
2. Use the assignment template (linked in Resources) for your lab screenshots and assignment responses.
3. Take screenshots from Lab 1, Section 1, Part 1: Step 5.
4. There are no screenshots required for Parts 2 and 3, but there are several questions to answer in your lab report.

Course Resources

Assignment Template [DOCX]

u06v1 - Learning Components

- Identify vulnerabilities that exist in a Web application.
- Identify tools that can be used to analyze Web servers, websites, and Web application tools.
- Identify vulnerabilities that exist in connection to the Internet.
- Identify vulnerabilities that exist on a website.

u06v2 - Lab: Performing Dynamic and Static Quality Control Testing

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

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

1. Follow the lab instructions carefully. Before beginning, review Sections 1 and 2.
2. Add your assignment responses to the assignment template you have in progress, remembering to label sections clearly. Note: there are no screenshots to take in this lab.

u06d1 - Vulnerability Scanning Tools

You are an IT security specialist recently hired to harden system security for a small boutique that operates a brick-and-mortar store and an e-commerce site. The store has six remote employees and 10 employees who work full time in the store. The Web server is housed in the basement of the storefront. You have decided to use a vulnerability scanner to test the Web server's vulnerabilities, but the owner is concerned about the cost. You have decided to prepare a comparison report to help her choose an appropriate tool. Describe the criteria you

will use to compare these tools and then provide a comparison report of three vulnerability scanning tools, one or more of which is open source, based on the selection criteria you used.

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide

u06d1 - Learning Components

- Identify tools that can be used to analyze Web servers, websites, and Web application tools.
- Describe what a vulnerability scan shows in its report.
- Describe the process for interpreting a Web vulnerability scan.

u06a1 - Website Vulnerabilities

By now, you should have completed the Evaluating Web Server Vulnerabilities and Performing Dynamic and Static Quality Control Testing labs for this unit and saved your screenshots in the assignment template.

Instructions

Consider your lab work and studies as you add your responses to the following in the assignment template:

- Describe briefly what you learned and observed in the two labs and include it in the section with your screenshots. Be specific in your response.
- Analyze the Skipfish report results you received in Lab 7, Section 3. Create a report to your CIO that identifies and discusses three of the critical vulnerabilities detected and the remediation strategy you would recommend.

Additional Requirements

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **Font and font size:** Times New Roman, 12 point.

Unit 7 >> Cyberoperations Overview

Introduction

The U.S. Joint Chiefs of Staff's 2018 *Joint Publication 3-12: Cyberspace Operations* defines *cyberspace* as the "Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networkee systems and associated physical infrastructures." *Cyberspace operations* (CO) is defined in this manual as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."

In this unit, you will examine cyberoperations at a high level and from the perspective of the United States' use of cyberoperations. You will be asked to reflect on the ethical impact of cyberoperations.

Reference

United States Joint Chiefs of Staff. (2018). *Joint publication 3-12: Cyberspace operations.* Retrieved from https://publicintelligence.net/jcs-cyberspace-operations/

Learning Activities

u07s1 - Studies

Readings

Use the Internet to complete the following:

- Goodman, R. (2018, Mar 8). Cyber operations and the U.S. definition of "armed attack" [Blog post]. Retrieved from https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/
- United States Joint Chiefs of Staff. (2018). Joint publication 3-12: Cyberspace operations [PDF]. Available from https://www.jcs.mil/
    - Read the Preface, Chapter 1, and Chapter 2.

u07s1 - Learning Components

- Describe cyberoperations.
- Describe cyber weapons.
- Identify legal and ethical issues related to offensive cyber weapons and cyberoperations.
- Identify international laws that apply to cyberoperations.
- Identify offensive cyberoperations.

u07d1 - Ethical Issues of Cyberoperations

Having read the first two chapters of the cyberspace operations report by the Joint Chiefs of Staff (linked in Resources), identify the aspect of cyberspace operations discussed in this publication that you found to have the most significant ethical implications and reasons for your choice. Discuss the integration of cyberoperations with on-the-ground military operations. How does the inclusion of cyberoperations enhance—and interfere with—current military operations?

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide
Joint Publication 3-12: Cyberspace Operations [PDF]

u07d1 - Learning Components

- Describe cyberoperations.
- Identify legal and ethical issues related to offensive cyber weapons and cyberoperations.
- Identify offensive cyberoperations.

u07d2 - Cyberoperations in the News

For this discussion, use the Internet to find a news article about a recent cyberoperations event. Summarize the article and be sure to include a link to it in your post. What are the implications of this incident for the United States and/or the world?

Response Guidelines

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

Course Resources

Graduate Discussion Participation Scoring Guide

u07d2 - Learning Components

- Describe cyberoperations.
- Describe cyber weapons.
- Identify legal and ethical issues related to offensive cyber weapons and cyberoperations.

Unit 8 >> Cyber Weapons

Introduction

This unit will introduce you to cyber weapons. A *cyber weapon* is computer hardware or software used to perform an act of cyber warfare, typically for a military or intelligence objective. Cyber weapons are usually associated with a state actor or terrorist group rather than organized crime. The unauthorized use of a cyber weapon by a human is an illegal act that could be considered an act of war. The cyber weapon performs an act that would typically be executed by a spy or soldier such as surveillance; data theft; data, hardware, or code destruction; or electromechanical or process-control systems damage. In this unit, you will explore examples of cyber weapons in various scenarios.

Learning Activities

u08s1 - Studies

Readings

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

- Adams, M., & Reiss, M. (2018, Mar 4). International law and cyberspace: Evolving views [Blog post]. Retrieved from https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views
- Bezsonoff, N. (2017, Aug 21). Your firewall won't save you from the next DDoS attack [Blog post]. Retrieved from https://www.itspmagazine.com/from-the-newsroom/your-firewall-wont-save-you-from-the-next-ddos-attack
- CFR Interactives. (2018). Cyber operations tracker. Retrieved from https://www.cfr.org/interactive/cyber-operations
- Cole, E. (2017). Offense must inform the defense – Is your cyber security program fixing the right problems. Retrieved from https://secure-anchor.com/offense-must-inform-defense/

- Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys, 51*(4), 1–36.
- Kilner, P. (2017, Dec 21). Ethics of cyber operations: '5th domain' creates challenges, needs new rules [Blog post]. Retrieved from https://www.ausa.org/articles/ethics-cyber-operations-%E2%80%985th-domain%E2%80%99-creates-challenges-needs-new-rules
- Pipyros, K., Thraskias, C., Mitrou, L., & Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers & Security,* 74, 371–383.

u08s1 - Learning Components

- Describe cyber weapons.
- Identify legal and ethical issues related to offensive cyber weapons and cyberoperations.
- Identify international laws that apply to cyberoperations.
- Identify offensive cyberoperations.

u08d1 - Cyber Weapon Scenario

You are the CIO for a large online retailer. The CEO and CFO have expressed concerns about vulnerability to cyber attacks such as distributed denial of service (DDoS) but they believe that the next-gen firewalls that were recently installed probably provide adequate protection. They want you to inform them thoroughly on the threat and potential mitigation for such an attack. You are aware of the "offense must inform the defense" approach to cybersecurity and intend to apply that approach to this problem.

For this discussion, address the following:

- How would you describe DDoS as a cyber weapon?
- In your opinion, based on research, does your organization fit the target type for DDoS attacks? Explain your response.
- What is the motivation for most DDoS attacks? Can your organization create this motivation for a DDoS attack? Explain.
- What type of DDoS attack would be most likely for this organization? Explain your response.
- What would you tell the CEO and CFO about the effectiveness of the current firewalls against a DDoS attack?
- Would you recommend a more offensive approach for this scenario? Explain and provide an example of an offensive approach. What are the legal and ethical implications of this approach?
- Which international laws might be relevant if this type of cyber attack occurred from a foreign agent?

Response Guidelines

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

substantive and appropriate responses.

Course Resources

Graduate Discussion Participation Scoring Guide

u08d1 - Learning Components

- Describe cyber weapons.
- Identify international laws that apply to cyberoperations.
- Identify offensive cyberoperations.

u08a1 - Cyberoperations

As we have discussed, cyber weapons may be used to render a computer or system inaccessible, intercept data, destroy an application or data, or damage devices attached to computers or systems. Ransomware is an example of an offensive use of a cyber weapon, in which a user's data is encrypted so the attacker can demand a ransom. Encryption is also used defensively to protect data confidentiality. We have seen offensive, covert cyberoperations used to influence elections and damage personal and professional reputations.

Instructions

After completing this week's readings, find a case related to the use of cyber weapons by a country other than the United States.

- Describe the case in terms of the weapon used, how it was used, the purpose of the offensive attack, and how the target responded to the attack.
- Discuss the motive of the attacker and what made the victim country an attractive target for this weapon.
- Analyze the state of international law with regard to this cyberoperation.
- Discuss any legal action taken by the country that was attacked.
- Indicate whether you would advise a country that has been attacked through a cyberoperation to retaliate with offensive cyber weapons. Justify your answer.
- Describe the ethical and legal implications of using offensive cyber weapons and cyberoperations against a state enemy.

Additional Requirements

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **Font and font size:** Times New Roman, 12 point.

Review the scoring guide to ensure that you meet all criteria before submitting your assignment.

Unit 9 >> Cyberoperation and Hacking Methods

Introduction

In this unit you will examine some of the core hacking methodologies currently in use. Hacking methodologies typically include the following phases:

1. Reconnaissance.
2. Scanning.
3. Infiltration.
4. Exfiltration.
5. Access extension.
6. Assault.
7. Obfuscation.

You will examine how hacking has evolved and discuss the laws and ethics relevant to hacking. You will then examine in detail sniffers, session hijacking, and denial of service attacks. *Sniffing* is the act of viewing communications on a network and intercepting sensitive information. The *session hijack* is a more advanced form of sniffing in which a hacker takes over an authenticated session. A denial of service attack involves a computer attacking another computer to shut it down and disallow any legitimate use of its operations. Finally, you will learn about botnets and the Internet of things (IoT).

Learning Activities

u09s1 - Studies

Readings

Use your *IAS5200: Network Architecture and Cyberoperations* custom text to read the following from Oriyano and Solomon's *Hacker Techniques, Tools, and Incident Handling*:

- Chapter 1, "Hacking: The Next Generation."
- Chapter 11, "Sniffers, Session Hijacking, and Denial of Service Attacks."

Use the Internet to read the following:

- Henry, J. (2018, Aug 6). 7 ways to identify darknet cybersecurity risks [Blog post]. Retrieved from https://securityintelligence.com/7-ways-to-identify-darknet-cybersecurity-risks/

Skillsoft Resources

Use the Capella library to complete the following:

- Behera, S. R. (2018). Chapter 18, Surface Web, deep Web, and dark net. In *Hacking exposed*, New Delhi, India: BPB Publications.
- CEHv10. (n.d.). *Hacking concepts* [Tutorial]. Skillsoft.
- CEHv10. (n.d.). *Wireless hacking common threats* [Tutorial]. Skillsoft.

u09s1 - Learning Components

- Research careers related to cyberoperations, ethical hacking, and reverse engineering.
- Identify specific roles and responsibilities required in the area of cyberoperations, ethical hacking, and reverse engineering.
- Research the educational background needed for careers in cyberoperations, ethical hacking, and reverse engineering.

u09d1 - Reducing Vulnerability to Hacking

For this discussion, read A Hacking Scenario: How Hackers Choose Their Victims (linked in Resources), then complete the following:

- Assume you work as an IT cybersecurity specialist for a large retailer. Based on what you have learned about how the typical hacker operates, what steps would you take to ensure that your system would not be vulnerable to this type of random hacker attack? Address each one of the hacker's actions.

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide
A Hacking Scenario: How Hackers Choose Their Victims [Blog post]

u09d1 - Learning Components

- Research careers related to cyberoperations, ethical hacking, and reverse engineering.
- Identify specific roles and responsibilities required in the area of cyberoperations, ethical hacking, and reverse engineering.
- Research the educational background needed for careers in cyberoperations, ethical hacking, and reverse engineering.

u09d2 - Protecting Data

For this discussion, consider the implications of a widespread virus that extracts data from hard drives and network databases and replaces it with gibberish. Assume that this virus has spread very rapidly across the United States and is now an epidemic, affecting businesses and individuals. U.S. Cert has requested that all business and personal users avoid logging on to their systems to slow the spread of the virus while the organization works to resolve the issue.

- How will inability to use networks affect businesses and individuals?
- What major daily functions for individuals and businesses would be impacted? Think about your daily activities and discuss the disruptions that would occur and how you would adapt.

Assume that your personal hard drive was infected and you have lost all data:

- Do you have a complete and current backup?
- Would that backup also be at risk?
- What steps could you take with your personal data to ensure its protection?

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide

u09d2 - Learning Components

- Identify specific roles and responsibilities required in the area of cyberoperations, ethical hacking, and reverse engineering.

Introduction

Having studied cyberoperations and cyber weapons in the last few units, in this unit we will explore emerging careers in the field of cyberoperations and cyber warfare, including the skills, certifications, and education required for them.

Learning Activities

u10s1 - Studies

Readings

Use the Internet to read the following:

- Aftergood, S. (2018, Jul 17). Secrecy news: Cyber war as a career path [Blog post]. Retrieved from https://fas.org/blogs/secrecy/2018/07/cyber-war-training/
- Baram, G. (2018, Jun 19). The theft and reuse of advanced offensive cyber weapons pose a growing threat [Blog post]. Retrieved from https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat

u10s1 - Learning Components

- Research careers related to cyberoperations, ethical hacking, and reverse engineering.
- Identify specific roles and responsibilities required in the area of cyberoperations, ethical hacking, and reverse engineering.
- Research the educational background needed for careers in cyberoperations, ethical hacking, and reverse engineering.

u10d1 - Cybersecurity Careers, Roles, and Responsibilities

You are the CIO for a large financial services firm. The business occupies eight floors of an office tower and has approximately 1000 employees. The organization's critical data center is housed in a basement. The database that stores confidential financial information is accessible at all times. A 99.9 percent uptime is required to prevent client and business revenue loss. The business's IT support comprises several network administrators and a network help-desk group. There are no security specialists on staff. The system includes Web servers, a database accessed by customers, field sales employees, and the internal staff. On-site backup mail and domain

servers exist. The organization has an alternative processing site 100 miles away that can hold 20 percent of the staff.

You and your staff are tasked with evaluating potential organizational impact of network failures on various scales, from one network device to the entire network going down. You must develop a risk mitigation plan to protect the business's critical business functions and critical business users. Your team is asked to address the following scenarios:

- CERT reports an active DDoS attack that is spreading. Due to this, the network administration team may need to close port 80 to incoming traffic in the near future.
- The CFO's workstation has been compromised by malware and some confidential and sensitive data may have been copied.
- A perimeter firewall has been configured incorrectly.

In your discussion post, address the following:

- Identify the IT cybersecurity roles needed on your team to address these and other scenarios effectively. Explain the need for each role.
- Choose one of the above scenarios. Discuss the impact to the organization and to its customers and mitigation strategies for the scenario.

Response Guidelines

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

Course Resources
Graduate Discussion Participation Scoring Guide

u10d1 - Learning Components

- Research careers related to cyberoperations, ethical hacking, and reverse engineering.
- Identify specific roles and responsibilities required in the area of cyberoperations, ethical hacking, and reverse engineering.
- Research the educational background needed for careers in cyberoperations, ethical hacking, and reverse engineering.

u10a1 - Careers in Cyberoperations, Ethical Hacking, and Reverse Engineering

As defensive and offensive cyberoperations continue to expand, reverse engineering is increasingly used for both applications. Assume you have completed your Master's degree at Capella and have decided to work in offensive or defensive cyberoperations, ethical hacking, or reverse engineering. Research job sites and on the Internet to determine what types of positions are available in these areas.

Write a paper in which you complete the following:

- Identify three job titles that interest you and describe the qualifications required, the type of organization posting the job, and the salary if indicated. Explain what interests you most about each role.
- Describe your responsibilities based on the job post.
- Of these jobs, identify the one for which you feel most qualified and explain why.
- List three interview questions that might be asked for one of these roles (cyberoperations, ethical hacking, or reverse engineering) and provide substantive answers to each.

Additional Requirements

- **Written communication:** Written communication is free of errors that detract from the overall message.
- **Font and font size:** Times New Roman, 12 point.

Before submitting your assignment, refer to the scoring guide to ensure that you meet all grading criteria.