Preview: IT4071 : Cyber Attacks and Ethical Hacking

Syllabus

Course Overview

Threats, vulnerabilities, and risks to systems, data, and buildings have been steadily increasing. Information technology security professionals are faced with constant challenges to secure network infrastructure. Organizations have lost business and reputation due to breaches and attacks from malicious insider threats and external attackers, especially cybercriminals.

In this course, we will explore systems and their components and employ hacking techniques and tools to identify specific vulnerabilities and threats. You will learn to use vulnerability management tools, penetration techniques, and cryptographic methods to assist in mitigating cybercrimes and cyber-attacks. The use of intrusion detection and intrusion prevention systems in ethical hacking and threat mitigation will also be explored.

Course Competencies

(Read Only)

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

1. Perform vulnerability analysis and penetration testing using ethical hacking techniques.
2. Describe the role of social engineering in gaining access to systems.
3. Analyze packets using sniffing tools.
4. Identify the vulnerabilities of common protocols used in an organization.
5. Design a plan for intrusion detection for a secure infrastructure.
6. Communicate in a manner that is professional and consistent with expectations for members of information technology professions.

Course Prerequisites

Prerequisite(s): IT3355, IT4803.

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

Oriyano, S-P. (2014). *Hacker techniques, tools, and incident handling* (2nd ed.). Burlington, MA: Jones & Bartlett Learning. ISBN: 9781284031713.

Miscellaneous Item

Validating your bookstore cart covers the cost for access to required labs directly linked in this course.

Oriyano, S-P. (2014). *Hacker techniques, tools, and incident handling* [Online labs]. Burlington, MA: Jones & Bartlett Learning. ISBN: 9781284141078.

Library

The following required readings are provided in the Capella University Library or linked directly in this course. To find specific readings by journal or book title, use Journal and Book Locator. Refer to the Journal and Book Locator library guide to learn how to use this tool.

- Bigger, D. (2014). CompTIA Network+ 2014: Firewalls and content filters [Video]. Skillsoft Ireland.
- Bigger, D. (2014). CompTIA Network+ 2014: Network command line tools [Video]. Skillsoft Ireland.
- Bigger, D. (2014). CompTIA Network+ 2014: Attack techniques [Video]. Skillsoft Ireland.
- Campbell, J. (2013). Networking fundamentals: Introduction to WHOIS [Video]. Skillsoft Ireland.
- Campbell, J. (2013). *Networking fundamentals: Introduction to wireless networks* [Video]. Skillsoft Ireland.
- Clarke, G. E. (2015). CSSLP: Cryptographic validation [Video]. Skillsoft Ireland.
- Dedam, C. (2017). ASP.NET: Prevent SQL injection attacks [Video]. Skillsoft Ireland.
- Giesenow, H. (2015). OWASP top 10: SQL server injection mitigation [Video]. Skillsoft Ireland.
- Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security*, *73*, 102–113.
- Hynes, B. (2012). Security essentials: Avoid social engineering attacks [Video]. Skillsoft Ireland.
- Hynes. B. (2012). Security essentials: Encrypting your wireless networks [Video]. Skillsoft Ireland.
- Kandel, E., & Selarnick, A. (2017). Insuring against social engineering attacks. *Risk Management*, *64*(5), 12, 14.
- Lachance, D. (2014). CompTIA Cloud+: Penetration testing and vulnerability assessment [Video]. Skillsoft Ireland.
- Lachance, D. (2014). CompTIA Cloud+: Telnet and nslookup [Video]. Skillsoft Ireland.
- Lachance, D. (2014). CompTIA CASP CAS-002: SQL injection [Video]. Skillsoft Ireland.
- Lachance, D. (2015). CISSP: Honeypots and honeynets [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Systems security certified practitioner: OSI and TCP/IP models [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Cryptography fundamentals: Describing cryptographic terminology [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Systems security certified practitioner: Participating in physical security operations [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity Analyst+: Honeypots [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Password cracking [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Exploring the Kali Linux suite of tools [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Linux OS monitoring tools [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Social engineering and phishing [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Wired and wireless networks [Video]. Skillsoft Ireland.
- Lachance, D. (2017). OWASP Top 10: A1 – Execute a SQL injection attack [Video]. Skillsoft Ireland.

- Lachance, D. (2017). Security Trends: Identifying social engineering attempts [Video]. Skillsoft Ireland.
- Lachance, D. (2017). Security trends: State sponsored hacking [Video]. Skillsoft Ireland.
- Lacoste, R. (2017). Security+: Introduction to physical security [Video]. Skillsoft Ireland.
- Lekies, S., Kotowicz, K., Groß, S., Vela Nava, E. A., & Johns, M. (2017, October and November). Code-reuse attacks for the Web: Breaking cross-site scripting mitigations via script gadgets. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1709–1723.
- Liu, S., Foster, I., Savage, S., Voelker, G. M., & Saul, L. K. (2015, October). Who is .com? Learning to parse WHOIS records. *IMC '15: Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, 369–380.
- Lobban, C. (2015). A+ practical: Physical security [Video]. Skillsoft Ireland.
- Miller, W. (2015). Defensive programming in Java: SQL injection attacks [Video]. Skillsoft Ireland.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates, and scenarios. *Computers and Security*, *59*, 186–209.
- Sampson, A. (2015). Securing user accounts: Protecting against password hacking [Video]. Skillsoft Ireland.
- Shannon, M. (2015). IINS: Social engineering [Video]. Skillsoft Ireland.
- Shannon, M. (2016). CISA: Security incident handling and response [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CompTIA CASP CS0-003: Reconnaissance, fingerprinting, & social engineering [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CompTIA CASP CS0-003: Penetration testing and assessment [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CISM: Components of an incident response plan [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CISM: Techniques to test the incident response plan [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CompTIA CASP CS0-003: Host-based IDS and IPS [Video]. Skillsoft Ireland.
- Shannon, M. (2017). Security+: Define social engineering and hijacking [Video]. Skillsoft Ireland.
- Shannon, M. (2017). Security+: Honeypots [Video]. Skillsoft Ireland.
- Shannon, M. (2017). Security+: Session hijacking [Video]. Skillsoft Ireland.
- Simms, I. (2016). Managing Citrix XenDesktop 7 solutions: Verifying DNS configuration [Video]. null
- Snyder, R. (2006, September). Ethical hacking and password cracking: A pattern for individualized security exercises. *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development*, 13–18.
- Sokol, P., Míšek, J., & Husák, M. (2017). Honeypots and honeynets: Issues of privacy. *EURASIP Journal on Information Security*, 4, 1–9.
- Welton, T. (2015). IT security for end users: Avoiding social engineering scams [Video]. Skillsoft Ireland.
- Welton, T. (2015). IT security for end users: Social engineering scam characteristics [Video]. Skillsoft Ireland.

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.

- Dayalan, M. (2017). Cyber risks: The growing threat. *International Journal of Novel Research and Development*, *2*(9), 4–6. Retrieved from http://www.ijnrd.org/viewpaperforall.php?paper=IJNRD1709002
- Offensive Security. (n.d.). What is Kali Linux? Retrieved from https://docs.kali.org/introduction/what-is-kali-linux
- SANS Institute. (n.d.). SANS reading room. Retrieved from https://www.sans.org/reading-room

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.

- Oriyano, S-P. (2014). *CEHv8: Certified ethical hacker version 8 study guide.* Indianapolis, IN: Sybex.

Unit 1 >> Hacking and Network Communications Basics

Introduction

Hacking encompasses many activities; likewise, the motivations of hackers may vary. Hackers can be divided into different categories based on permission, motivation, and skill. There are many different techniques a hacker may choose to employ depending on their goals and ability. Regardless, all hackers employ a similar methodology.

Hacking done with explicit permission to test the security of a network is called penetration testing. Penetration testers require many skills and practitioners must have a basic understanding of network protocols. This week's assignment will also discuss the transmission control protocol/Internet protocol (TCP/IP).

Learning Activities

Required Readings

Use your *Hacker Techniques, Tools, and Incident Handling* text to read the following:

- Chapter 1, "Hacking: The Next Generation," pages 2–22.
- Chapter 2, "TCP/IP Review," pages 23–49.

Use the Internet to read the following:

- Dayalan, M. (2017). Cyber risks: The growing threat. *International Journal of Novel Research and Development*, *2*(9), 4–6. Retrieved from http://www.ijnrd.org/viewpaperforall.php?paper=IJNRD1709002

Required Skillsoft Videos

For this unit, complete the following:

- Lachance, D. (2017). Security trends: State sponsored hacking [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CompTIA CASP CS0-003: Penetration testing and assessment [Video]. Skillsoft Ireland.
- Lachance, D. (2014). CompTIA Cloud+: Penetration testing and vulnerability assessment [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Systems security certified practitioner: OSI and TCP/IP models [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following readings in *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning:

- Chapter 1, "Getting Started With Ethical Hacking."
- Chapter 2, "System Fundamentals."

Capella's Skillsoft library guide provides support on searching Skillsoft and working with its results.

Technical Support for Skillsoft

Capella provides Academic Technical Support to help learners with technical issues in courses. Visit Technical Support if you have any issues with the Skillsoft resources.

- Examine core concept and principles for assessing and securing systems on a Wide Area Network.
- Analyze how to apply encryption and hashing algorithms for secure communications.
- Practice commands and procedures required to assess and secure systems on a Wide Area Network.
- Practice applying key concepts and procedures involved in applying encryption and hashing algorithms for secure communications.

u01a1 - Assessing and Securing Systems on a Wide Area Network (WAN)

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Assessing and Securing Systems on a Wide Area Network (WAN) lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. Which Nmap command, including the switches used, did the lab require you to run first?
  2. Describe which ports were determined to be open, including service names after scanning 100.16.16.50 with Nmap.
  3. You have been asked to run a vulnerability scan against 100.20.9.25. What command would you use to perform an MS08-067 vulnerability scan?
  4. Describe the MS08-067 vulnerability and explain why it is so important to take steps to mitigate this vulnerability.
  5. Identify the operating systems of each of the IP addresses scanned during the Nmap lab.

Refer to the Assessing and Securing Systems on a Wide Area Network (WAN) scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u01d1 - Ethical Hacking Roles and Vulnerability Management (C1)

Introduction

The term *hacker* has changed over the years and might be difficult to categorize. Likewise, the reasons for hacking are myriad. Understanding some of the most common reasons for hacking is important in defensive efforts. For example, the motivations of a hacker interested in correcting a social wrong are much different from those who use hacking as an expansion of a criminal enterprise, even if their techniques are similar. Understanding these different motivations is key to protecting an environment against attack.

An information technology professional can use skills and techniques acquired from troubleshooting operating systems and applications, and an understanding of the mindset of a hacker, to become an effective ethical hacker.

Instructions

Initiate a discussion of your concepts, ideas, and thoughts on three different groups of hackers and explain their motivations.

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners during the course.

Your initial post should be between 150–200 words and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses should be 75–100 words and are due by 11:59 p.m. CST on Sunday.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u01d2 - Laws on Ethical Hacking and Penetration Testing (C1)

Introduction

Ethical hackers are individuals who break into systems legally and ethically to detect vulnerabilities and determine threats that malicious outside hackers or malicious inside attackers can exploit.

Ethical hackers are bound by strict rules governing their behavior, while other types of hackers face no such constraints. The ethical hacker must work hard to earn and maintain trust. Further, since ethical hackers are placed in a position of great trust, they must always carefully consider their actions to ensure they are following the rules. Breaking the rules erodes trust and in some cases may be illegal. For these reasons, it is important for an ethical hacker to adhere to a strict code of ethics and to be knowledgeable about local laws regarding their activities.

Cases exist where an ethical hacker has become a gray hat hacker and subsequently a black hat hacker. This type of transition leaves organizations highly vulnerable. Loss of trust and legal implications are two of the major aspects that an ethical hacker should consider when breaking the rules and regulations of ethical hacking.

Instructions

Initiate a discussion of your concepts, ideas, and thoughts on three major regulations, laws, or directives that an ethical hacker should know.

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners during the course.

Your initial post should be between 150–200 words and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses should be 75–100 words and are due by 11:59 p.m. CST on Sunday.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u01v1 - Lab: Assessing and Securing Systems on a Wide Area Network (WAN)

Read the list of questions in this unit's assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources
Lab: Assessing and Securing Systems on a Wide Area Network (WAN).

Unit 2 >> Cryptography and Physical Security: Two Essential Components of Securing the Enterprise

Introduction

In this week's lesson, we discuss two methods that are essential components in securing an enterprise: encryption and physical security. Encryption is often used on Web pages, e-mail, and virtual private networks (VPNs). It is crucial for security professionals to have at least a rudimentary knowledge of cryptography and cryptanalysis.

Physical security is another crucial, if often overlooked, component of security. Physical security involves a diverse range of controls such as hard-drive encryption, media sanitation methods, lighting, fences, and locks.

Learning Activities

Required Readings

Use your *Hacker Techniques, Tools, and Incident Handling* text to read the following:

- Chapter 3, "Cryptographic Concepts," pages 50–82.
- Chapter 4, "Physical Security," pages 83–106.

Required Skillsoft Videos

For this unit, complete the following:

- Clarke, G. E. (2015). CSSLP: Cryptographic validation [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Cryptography fundamentals: Describing cryptographic terminology [Video]. Skillsoft Ireland.
- Lacoste, R. (2017). Security+: Introduction to physical security [Video]. Skillsoft Ireland.
- Lobban, C. (2015). A+ practical: Physical security [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Systems security certified practitioner: Participating in physical security operations [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional reading from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 3, "Cryptography."

Technical Support for Skillsoft

Capella provides Academic Technical Support to help learners with technical issues in courses. Visit the Technical Support if you have any issues with the Skillsoft resources.

u02s1 - Learning Components

- Analyze how to apply encryption and hashing algorithms for secure communications.
- Analyze hybrid website attacks.
- Practice applying key concepts and procedures involved in applying encryption and hashing algorithms for secure communications.
- Analyze different types of attack strategies that attackers may employ.
- Analyze mitigation strategies for each type of attack.

- Evaluate different strategies for preventing and mitigating a hybrid attack.

u02s2 - Assignment Preparation

In the second assignment in Unit 2, you will be asked to create a PowerPoint presentation for senior management to address the problem of a hybrid attack on a website. Take time now to review the assignment description and scoring guide.

Then begin preparing for the assignment by researching and analyzing existing IT literature for articles on the following topics:

- Different types of attack strategies hackers may employ in a hybrid website attack, including at least eight of the Web-based attack strategies listed below:
  - Cross-site scripting (XSS) attack.
  - Cross-site request forgery (CSRF).
  - SQL injection.
  - Code injection.
  - Command injection.
  - Parameter tampering.
  - Cookie poisoning.
  - Buffer overflow.
  - Cookie snooping.
  - DMZ protocol attack.
  - Zero-day attack.
  - Authentication hijacking.
  - Log tampering.
  - Directory traversal.
  - Cryptographic interception.
  - URL interpretation.
  - Impersonation attack.
- Mitigation strategies for each type of attack and the effectiveness of each of those strategies.

Your assignment must be supported by a minimum of four recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Use the Internet and the Capella University Library Journal and Book Locator for your research.

Use the Journal and Book Locator Library Guide to assist in your research.

u02s2 - Learning Components

- Analyze hybrid website attacks.

- Analyze different types of attack strategies that attackers may employ.
- Analyze mitigation strategies for each type of attack.
- Evaluate different strategies for preventing and mitigating a hybrid attack.

u02a1 - Applying Encryption and Hashing Algorithms for Secure Communications

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Applying Encryption and Hashing Algorithms for Secure Communications lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. Explain why hash values are an important part of performing a forensic investigation.
  2. Do hash values typically change if data is modified? Explain why or why not.
  3. List a method of securing message integrity during e-mail communications without encrypting the e-mail.
  4. Explain the purpose of the –e switch in the GnuPG command.
  5. Compare and contrast MD5sum and SHA1sum hashing algorithms.
  6. During the lab, several cryptographic algorithms were used. Name them.
  7. Explain what is required to decrypt an encrypted message.
  8. Explain the purpose of the –d switch in the GnuPG command.
  9. List some ways to create entropy in a GnuPG encryption key.

Refer to the Applying Encryption and Hashing Algorithms for Secure Communications scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u02a2 - Web-Based Attacks

Introduction

Cybercriminals have orchestrated a hybrid attack on your city's municipal website. The Federal Bureau of Investigation (FBI) has asked that the municipal website be taken offline and that infrastructure that supports the website be isolated until a thorough investigation has been completed. You have been asked to create a PowerPoint presentation for senior management to address the problem.

Instructions

In your presentation, you will need to:

1. Describe different types of attack strategies attackers may employ.
2. Evaluate mitigation strategies for each type of attack.
3. Recommend a course of action for addressing the Web attack.
4. Support your presentation with a minimum of four references.
5. Communicate in a manner that is highly professional and consistent with expectations for professionals in the field of information technology.

Your presentation must:

- Include a minimum of 16–18 slides, along with extensive speaker notes (see Submission Requirements, below).
- Address at least eight of the Web-based attack strategies listed below:
    - Cross-site scripting (XSS) attack.
    - Cross-site request forgery (CSRF).
    - SQL injection.
    - Code injection.
    - Command injection.
    - Parameter tampering.
    - Cookie poisoning.
    - Buffer overflow.
    - Cookie snooping.
    - DMZ protocol attack.
    - Zero-day attack.
    - Authentication hijacking.
    - Log tampering.
    - Directory traversal.
    - Cryptographic interception.
    - URL interpretation.
    - Impersonation attack.

Structure your presentation as follows:

- Title (one slide).

- Introduction (two slides): Identify the problem and list the Web-attack strategies you have chosen to address.
- Main slides (a minimum of eight slides): On each slide, describe one of the possible attack strategies and analyze possible mitigation strategies.
- Recommended course of action (1–2 slides).
- References on the final slide (a minimum of one slide).

Tips for your slide presentation:

- Use the speaker notes to include the information you want to share with your audience. The speaker notes must be coordinated with the information on the slides.
- Be sure to provide APA-formatted citations for your sources.
- Be creative. You can add audio to the presentation if you choose to do so; however, it is not required.

Capella academic integrity standards must be strictly followed.

Submission Requirements

- **PowerPoint presentation:** Should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Number of slides:** 16–18 slides. Information in the slides should be in bulleted list format with a minimum of four bullets per slide.
- **Speaker notes:** Include a minimum of 100–150 words for each main slide. The information in the speaker notes must contain at least one reference per slide. Double-spaced the lines.
- **References:** Include a minimum of four recent, peer-reviewed references.
- **APA style:** References and citations should be formatted using current APA style.
- **Font for slides:** Times New Roman, 28–32 points.
- **Font for speaker notes:** Times New Roman, 12 points.

Course Resources
Journal and Book Locator Library Guide
Journal and Book Locator
APA Style and Formatting

u02d1 - Cryptography and Vulnerability Management (C1)

Introduction

Encryption is used to provide confidentiality, integrity, and non-repudiation, to name a few. Three main types of encryption are symmetric encryption, asymmetric encryption, and hashing algorithms. There are advantages associated with each method and they are often combined to provide the most benefit. Although encryption can be used to increase security, it also requires processing power to perform. Security professionals must carefully balance the cost of encryption versus the risk of not encrypting to determine the most appropriate approach for their environment.

Instructions

You have been working long hours and have been taking work home on an external USB drive. Much of the work you do involves proprietary company information. You place your USB drive in your pocket and head out. On the way to work, you stop by a restaurant to grab a quick bite to eat before another long day. When you get to work you realize the USB drive is no longer in your pocket. You carefully check your car and still cannot find it.
You realize you must have dropped it earlier. You go back to the restaurant and the USB drive is not there. The data on the USB drive was encrypted. Do you need to be concerned with losing the USB drive? Does the type of encryption used matter; why or why not?

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners.

Your initial post should be between 150–200 words and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses should be 75–100 words and are due by 11:59 p.m. CST on Sunday.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u02v1 - Lab: Applying Encryption and Hashing Algorithms for Secure Communications

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Applying Encryption and Hashing Algorithms for Secure Communications.

Unit 3 >> Footprinting Tools and Techniques

Introduction

Footprinting, or reconnaissance, is the first phase of hacking. It involves the passive gathering of information about the intended target. The methods of gathering data include a diverse range of activities such as getting data from a company website or social media, Google hacking, and using dynamic name system (DNS) information. The time invested during this phase can be used by the hacker to increase the effectiveness of an attack. An understanding of how attackers use footprinting techniques can allow security practitioners to make it more difficult for attackers to prevail.

Learning Activities

u03s1 - Studies

Required Readings

Use your *Hacker Techniques, Tools, and Incident Handling* text to read the following:

- Chapter 5, "Footprinting Tools and Techniques," pages 108–138.

Use the Capella library to read the following:

- Liu, S., Foster, I., Savage, S., Voelker, G. M., & Saul, L. K. (2015, October). Who is .com? Learning to parse WHOIS records. *IMC '15: Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, 369–380.

Required Skillsoft Videos

For this unit, complete the following:

- Lachance, D. (2014). CompTIA Cloud+: Telnet and nslookup [Video]. Skillsoft Ireland.
- Bigger, D. (2014). CompTIA Network+ 2014: Network command line tools [Video]. Skillsoft Ireland.
- Simms, I. (2016). Managing Citrix XenDesktop 7 solutions: Verifying DNS configuration [Video].
- Campbell, J. (2013). Networking fundamentals: Introduction to WHOIS [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional readings from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 4, "Footprinting and Reconnaissance."
- Chapter 7, "Gaining Access to a System."

Technical Support for Skillsoft

Capella provides Academic Technical Support to help learners with technical issues in courses. Visit the Technical Support if you have any issues with the Skillsoft resources.

u03s1 - Learning Components

- Analyze data gathering and footprinting.
- Practice using concepts and procedures involved in data gathering and footprinting.

u03s2 - Assignment Preparation

In the second assignment in Unit 3, Tools to Explore Domain Information, you will be asked to write an assignment on footprinting. Take time now to review the assignment description and scoring guide.

Then begin preparing for the assignment by researching and analyzing existing IT literature for information on the following topics:

- The most common tools used by both malicious and ethical hackers to conduct footprinting.
- Reasons why ethical hackers explore network information before carrying out an investigation.
- The primary differences between Nslookup and Whois in assessing domain information.
- How an ethical hacker uses the information derived by use of Nslookup and Whois to mitigate network connectivity issues.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Use the Internet and the Capella University Library Journal and Book Locator for your research.

Use the Journal and Book Locator Library Guide to assist in your research.

u03s2 - Learning Components

- Analyze data gathering and footprinting.
- Practice using concepts and procedures involved in data gathering and footprinting.
- Analyze the most common tools used by both malicious and ethical hackers to conduct footprinting.
- Discuss why ethical hackers explore network information before carrying out an investigation.
- Research the primary differences between Nslookup and Whois in assessing domain information.
- Analyze how an ethical hacker uses the information derived by use of nslookup and Whois to mitigate network connectivity issues.

u03a1 - Data Gathering and Footprinting on a Targeted Website

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the lab linked below.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. Explain why the Whois tool is useful.

2. List some useful functions that are included in Sam Spade. Which do you think you will be mostly likely to use?
3. Explain what output is generated by the tracert command. Provide a scenario where you might use tracert as an investigative tool.
4. Provide a brief description of Sam Spade. Do you think Sam Spade is useful to security practitioners? Do you think hackers might find Sam Spade equally useful?
5. Discuss the privacy considerations in regards to Whois information.
6. Describe the purpose of footprinting.
7. List the primary technical contacts for the three domains discussed in your lab.

Refer to the Data Gathering and Footprinting on a Targeted Website scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u03a2 - Tools to Explore Domain Information

Introduction

During your reading this week, you learned about the significance of footprinting to hackers. Hackers take everyday information and network tools and distort their purpose to aid in their hacking activities. They compile the information they learn during the footprinting phase to increase the effectiveness of their attacks. Understanding how attackers use these tools is an important first step in mitigating attacks.

Instructions

In this assignment, write a 4–5 page paper in which you:

- Describe the most common tools used by both malicious and ethical hackers to conduct footprinting.
- Describe why ethical hackers explore network information before carrying out an investigation.
- Analyze the primary differences between Nslookup and Whois in assessing domain information.
- Explain how an ethical hacker uses the information derived by use of Nslookup and Whois to mitigate network connectivity issues.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Structure your report as follows:

- Title page.
- Introduction.
- The main body (at least three pages); use headings to identify individual sections.
- Summary and conclusion.
- References page.

Capella academic integrity standards must be strictly followed.

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional
- **References:** Include a minimum of three recent, peer-reviewed references.
- **APA style:** Citations and references must be formatted using current APA style.
- **Length of the report:** A minimum of four typed, double-spaced pages, excluding the title page and references page.
- **Font:** Times New Roman, 12 points.

Course Resources
Journal and Book Locator
Journal and Book Locator Library Guide

u03v1 - Lab: Data Gathering and Footprinting on a Targeted Website

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Data Gathering and Footprinting on a Targeted Web Site.

Unit 4 >> Port Scanning, Enumeration, and Wireless Vulnerabilities

Introduction

Last week, we discussed footprinting. This week, we move on to port scanning, followed by enumeration and, finally, wireless vulnerabilities.

Port scanning allows an attacker to learn what devices and services are used within an environment and thus exposes potential vulnerabilities. Enumeration expands upon the information already gathered before the hacker launches the actual attack. Port scanning is an essential step in compromising both wired and wireless networks; however, networks that use wireless are particularly susceptible because an attacker only needs proximity to the network to perform hacking activities.

Learning Activities

u04s1 - Studies

Required Readings

Use your *Hacker Techniques, Tools, and Incident Handling* text to read the following:

- Chapter 6, "Port Scanning," pages 139–161.
- Chapter 7, "Enumeration and Computer System Hacking," pages 162–189.

- Chapter 8, "Wireless Vulnerabilities," pages 190–214.

Required Skillsoft Videos

For this unit, complete the following:

- Campbell, J. (2013). Networking fundamentals: Introduction to wireless networks [Video]. Skillsoft Ireland.
- Hynes. B. (2012). Security essentials: Encrypting your wireless networks [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Wired and wireless networks [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional readings from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 5, "Scanning Networks."
- Chapter 17, "Physical Security."

Technical Support for Skillsoft

Capella provides Academic Technical Support to help learners with technical issues in courses. Visit the Technical Support if you have any issues with the Skillsoft resources.

u04s1 - Learning Components

- Analyze how a hacker can use ethical hacking techniques to exploit a vulnerable workstation.
- Practice using key ethical hacking concepts and techniques.

u04s2 - Assignment Preparation

In the second assignment in Unit 4, Discovery and Mitigation of Threats, you will be asked to write a report for senior management on how to address host-to-host threats. Take time now to review the assignment description and scoring guide.

Then begin preparing for the assignment by researching and analyzing existing IT literature for articles on the following topics:

- Procedures and tools used to discover port scanning threats and systems impacted.
- Procedures and tools used to discover used to discover session hijacking threats and systems impacted.
- Procedures and tools for mitigating these threats, including:

a. Secure Socket Layer.
b. Transport Layer Security.
c. Advanced Encryption Standard (AES) 256.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Use the Internet and the Capella University Library Journal and Book Locator for your research.

Use the Journal and Book Locator Library Guide to assist in your research.

u04s2 - Learning Components

- Analyze host-to-host threats.
- Analyze procedures and tools used to discover the port scanning threats and the systems impacted.
- Analyze procedures and tools used to discover the session hijacking threats and the systems impacted.
- Analyze procedures and tools for mitigating host-to-host threats, including: a) Secure Socket Layer, b) Transport Layer Security, c) Advanced Encryption Standard (AES) 256.

u04a1 - Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. List the stages of ethical hacking and provide a brief description of each.
  2. List the open ports and corresponding services discovered by Zenmap during your lab.
  3. During which stage of ethical hacking would you be most likely to use Zenmap?
  4. During which stage of ethical hacking would know vulnerabilities be identified?
  5. What vulnerability was discovered during your scan of the Linux system?
  6. What is the first thing you must do before performing ***any*** vulnerability test?

Refer to the Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u04a2 - Discovery and Mitigation of Threats

Introduction

Human threats such as theft, terrorism, and malicious insider attacks are considered significant threats to XYZ Corporation, a multi-national company located in Las Vegas, Nevada. The international information technology security team has recently discovered host-to-host threats using footprinting techniques such as port scanning and session hijacking.

The IT security team decided to use host-to-host security protocols such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) to mitigate the host-to-host threats. However, the cybersecurity blue team recommends the implementation of a symmetric algorithm such as Advanced Encryption Standard (AES) 256 to protect data in XYZ Corporation.

Instructions

The chief information security officer (CISO) has requested that you write a 5–7 page report to describe how the threats were discovered and evaluate approaches for mitigating them.

Your report must:

1. Describe procedures and tools (most likely) used to discover the port scanning threats and the systems impacted.
2. Describe procedures and tools (most likely) used to discover the session hijacking threats and the systems impacted.
3. Evaluate procedures and tools for mitigating these threats, including:
    a. Secure Socket Layer.
    b. Transport Layer Security.
    c. Advanced Encryption Standard (AES) 256.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Structure your report as follows:

- Title page.
- Introduction.
- The Main body (at least five pages); use headings to identify individual sections.
- Summary and conclusion.
- References page.

Capella academic integrity standards must be strictly followed.

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional
- **References:** Include a minimum of three recent, peer-reviewed references.
- **APA style:** Citations and references must be formatted using current APA style.
- **Length of the report:** A minimum of five typed, double-spaced pages, excluding the title page and references page.
- **Font:** Times New Roman, 12 points.

Course Resources
Journal and Book Locator Library Guide
Journal and Book Locator

u04d1 - Detection of Host Machines and Wireless Ethical Hacking

Introduction

Wireless networks can pose a risk to the enterprise because they can be used as a route into the wired network. Each legitimate wireless network is another potential attack vector. Rogue access points pose an even greater risk because they may provide a conduit for an attacker to gain entrance to a network or may be used to trick a victim into thinking they are connecting to a legitimate network. In either case, the ability to identify and locate rogue access point is an important skill for any security practitioner.

Instructions

Numerous complains been received by the chief information security officer (CISO) concerning the availability of rogue wireless devices in your network. These unauthorized connections utilize network resources and expose

the organization to vulnerabilities and threats. The CISO asked you to detect hosts in the internal network with the unsupported wireless network interface.

In this discussion:

- Name and describe at least two wireless ethical hacking tools that can be used to accomplish the CISO's request.
- Describe a strategy can you use to protect the organization from attacks that can be levied through rogue wireless access points.

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners.

Your initial post should be between 150–200 words and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses should be 75–100 words and are due by 11:59 p.m. CST on Sunday.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u04v1 - Lab: Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation.

Unit 5 >> Web and Database Attacks

Introduction

Most organizations rely on a Web presence to conduct business; likewise, attackers frequently find websites a lucrative target. In some cases, attackers attempt to exfiltrate data, while in other cases, a website is used as an attacker's entry point onto the local area network (LAN). In yet other cases, attackers just want to compromise the availability of the website. Many websites are supported by a backend database. This database is often of more interest to the attacker than the actual website. Security professionals must use a variety of strategies to secure the websites under their control; however, finding the balance between accessibility and security may be challenging.

Learning Activities

u05s1 - Studies

Required Resources

Use your *Hacker Techniques, Tools, and Incident Handling* text to complete the following:

- Review Chapter 7, "Enumeration and Computer System Hacking," pages 162–189.
- Read Chapter 9, "Web and Database Attacks," pages 215–239.

Use the Capella library to read the following:

- Snyder, R. (2006, September). Ethical hacking and password cracking: A pattern for individualized security exercises. *InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development*, 13–18.
- Lekies, S., Kotowicz, K., Groß, S., Vela Nava, E. A., & Johns, M. (2017, October and November). Code-reuse attacks for the Web: Breaking cross-site scripting mitigations via script gadgets. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1709–1723.

Required Skillsoft Videos

For this unit, complete the following:

- Miller, W. (2015). Defensive programming in Java: SQL injection attacks [Video]. Skillsoft Ireland.
- Dedam, C. (2017). ASP.NET: Prevent SQL injection attacks [Video]. Skillsoft Ireland.
- Lachance, D. (2017). OWASP Top 10: A1 – Execute a SQL injection attack [Video]. Skillsoft Ireland.
- Giesenow, H. (2015). OWASP top 10: SQL server injection mitigation [Video]. Skillsoft Ireland.
- Lachance, D. (2014). CompTIA CASP CAS-002: SQL injection [Video]. Skillsoft Ireland.
- Sampson, A. (2015). Securing user accounts: Protecting against password hacking [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Password cracking [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional readings from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 6, "Enumeration of Services."
- Chapter 13, "Web Servers and Web Applications."
- Chapter 14, "SQL Injection."

u05s1 - Learning Components

- Analyze how hackers attack vulnerable web applications and databases.
- Practice using key concepts and procedures involved in attacking vulnerable web applications and databases.

u05s2 - Assignment Preparation

In the second assignment in Unit 5, Vulnerabilities of Web Servers, you will be asked to write an assignment on web security. Take time now to review the assignment description and scoring guide.

Begin preparing for the assignment by researching and analyzing existing IT literature for information on the following topics:

- Cross-site scripting (CSS).
- Cross-site request forgery (CSRF).
- Buffer overflow.
- Structured query language (SQL) injection attacks.
- Types of attacks used by hackers to attack database management systems.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Use the internet and the Capella University Library Journal and Book Locator for your research.

Use the Journal and Book Locator Library Guide to assist in your research.

u05s2 - Learning Components

- Research cross-site scripting (CSS), cross-site request forgery (CSRF), buffer overflow, and structured query language (SQL) injection attacks.
- Analyze the differences between cross-site scripting (CSS) and cross-site request forgery (CSRF).
- Analyze the differences between buffer overflow with structured query language (SQL) injection attacks.
- Research which types of attacks are used by hackers to attack database management systems.

u05a1 - Attacking a Vulnerable Web Application and Database

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Attacking a Vulnerable Web Application and Database lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. When should the initial penetration test be performed on a web server? Why?
  2. Compare and contrast a cross-site scripting attack and a reflective cross-site scripting attack.
  3. What Web application attacks are most likely to compromise confidentiality?
  4. What techniques can you use to mitigate and respond to SQL injection attacks?

5. List some common techniques to identify Web application server vulnerabilities.
6. Discuss your plan for ensuring penetration and web application testing are part of the implementation process.
7. Why were you asked to set the DVWA security level to low during your lab?

Refer to the Attacking a Vulnerable Web Application and Database scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u05a2 - Vulnerabilities of Web Servers

Introduction

Attackers target websites for many different reasons. For example, an attacker may want to compromise the backend of an e-commerce website or take a site down using a denial of service or buffer overflow attacks. In fact, the attacker may be targeting your site's visitors. Since it may be difficult to anticipate an attacker's motivation, sites should be hardened to prevent as many types of attacks as possible.

Instructions

You were asked to participate with senior management in a Web conference discussing Web security. One speaker in correctly discussed installed SSL certificates, misconfiguration of Web servers, lack of server hardening, and poor authentication mechanisms as the most common threats to Web security. Another speaker added that the lack of security policy was the biggest risk. Then a Web developer discussed the threats posed by cross-site scripting (CSS), cross-site request forgery (CSRF), and buffer overflow. Finally, the last presenter discussed structured query language (SQL) injection attacks.

After the conference, the chief information security officer (CISO) of your organization asked you to write a report to summarize the information discussed during the conference.

Write a 4–5 page report in which you:

- Describe cross-site scripting (CSS), cross-site request forgery (CSRF), buffer overflow, and structured query language (SQL) injection attacks
- Compare cross-site scripting (CSS) and cross-site request forgery (CSRF).
- Compare buffer overflow, and structured query language (SQL) injection attacks.
- Discuss which attacks are used by hackers to attack database management systems.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Structure your report as follows:

- Title page.
- Introduction.
- The Main body (at least four pages); use headings to identify individual sections.
- Summary and conclusion.
- References page.

Capella academic integrity standards must be strictly followed.

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional
- **References:** Include a minimum of three recent, peer-reviewed references.
- **APA style:** Citations and references must be formatted using current APA style.
- **Length of the report:** A minimum of four typed, double-spaced pages, excluding the title page and references page.
- **Font:** Times New Roman, 12 points.

Course Resources
Journal and Book Locator
Journal and Book Locator Library Guide

u05d1 - Password Cracking

Introduction

Good password hygiene is an important component of securing any network. Attackers often attempt to compromise passwords. For this reason, it is good practice to use a unique password for each website, service, and application. Attackers have specialized tools to assist in cracking passwords; however, some passwords are more difficult to crack than others. Constructing unique, secure passwords may be challenging but some of this difficulty can be alleviated by using a password keeper.

Instructions

You have been monitoring the traffic on your network using passive sniffing tools such as EtherApe, Dsniff, and Omnipeek. During your analysis, you notice a large amount of interesting traffic coming from two unknown devices. The devices have been isolated on a decoy network. You are asked to see if you can compromise the unknown devices using a password cracking tool so that you can gain a better understanding of the attackers' intentions.

In your discussion post:

- Describe three password cracking tools you can use to access the suspected computers without the attackers' knowledge.
- Compare and contrast the different password cracking tools.

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners.

Your initial post should be between 150–200 words in length and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses should be 75–100 words in length and are due by 11:59 p.m. CST on Sunday.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u05v1 - Lab: Attacking a Vulnerable Web Application and Database

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Attacking a Vulnerable Web Application and Database.

Unit 6 >> Sniffers, Session Hijacking, and Denial of Service Attacks

Introduction

Sniffing, session hijacking, and denial of services (DoS) attacks are a threat to network security. Combined, these attacks compromise the confidentiality, integrity, and availability of the network. Sniffing is used to view network transmissions and is seen as a threat to confidentiality. Conversely, session hijacking is a threat to data integrity because an attacker can modify the data of the victim. Lastly, DoS attacks affect the availability of the network. Understanding these attacks will allow you to prepare appropriate mitigation strategies.

Learning Activities

u06s1 - Studies

Required Readings

Use your *Hacker Techniques, Tools, and Incident Handling* text to read the following:

- Chapter 11, "Sniffers, Session Hijacking, and Denial of Service Attacks," pages 278–300.

Required Skillsoft Videos

For this unit, complete the following:

- Shannon, M. (2017). Security+: Session hijacking [Video]. Skillsoft Ireland.
- Bigger, D. (2014). CompTIA Network+ 2014: Attack techniques [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional readings from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 8, "Trojans, Viruses, Worms, and Covert Channels."
- Chapter 9, "Sniffers."
- Chapter 11, "Denial of Service."
- Chapter 12, "Session Hijacking."

u06s1 - Learning Components

- Analyze how to identify and remove malware on a Windows system.
- Practice using key concepts and procedures for identifying and removing malware on a Windows systems.

u06s2 - Assignment Preparation

In the second assignment in Unit 6, Denial of Service, you will be asked to write a report for senior management on Denial of Service (DoS) attacks. Take time now to review the assignment description and scoring guide.

Then begin preparing for the assignment by researching and analyzing existing IT literature for articles on the following topics:

- Definitions of DoS and DDoS attacks.

- Differences between denial of service (DoS) attacks and distributed denial of service (DDoS) attacks.
- The relationship between DDoS attacks and botnets.
- How ethical hackers use DoS or DDoS to assess the damage caused by malicious hackers.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Use the internet and the Capella University Library Journal and Book Locator for your research.

Use the Journal and Book Locator Library Guide to assist in your research.

u06s2 - Learning Components

- Research DoS and DDoS attacks.
- Discuss the differences between denial of service (DoS) attacks and distributed denial of service (DDoS) attacks.
- Analyze the relationship between DDoS attacks and botnets.
- Research how ethical hackers use DoS or DDoS to assess the damage caused by malicious hackers.

u06a1 - Identifying and Removing Malware on a Windows System

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Identifying and Removing Malware on a Windows System lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. What is the significance of updating antivirus software signatures before performing a scan?
  2. List some characteristics of a computer that has been compromised.
  3. Where is malware moved to by AVG Antivirus Business Edition?
  4. List the contents of the Virus Vault referenced in your lab.
  5. Compare and contrast a complete scan with Resident Shield.

Refer to the Identifying and Removing Malware on a Windows System scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u06a2 - Denial of Service

Introduction

Denial of service (DoS) attacks are a threat to system security. These attacks consume system resources, network resources, and exploit programming flaws to stop legitimate system use. Distributed denial of service (DDoS) attacks use multiple computers to increase the intensity of the attack. For example, an attacker might use a botnet, consisting of many compromised computers, to launch an attack against a corporate e-commerce site, costing the company revenue.

Instructions

A recent cyber-attack has left your Web servers unresponsive, essentially closing your online store for business. You are losing revenue every minute your site is down, and you need to stop the bleeding quickly. An analysis of the attack revealed a high consumption of system resources, high network utilization, and exploitation of programming defects.

The chief information security officer (CISO) of your organization has asked you to write a report how the attack may have been implemented.

Write a 4–5 page report in which you:

- Define DoS and DDoS attacks.
- Analyze the differences between DoS and DDoS attacks.
- Describe the relationship between DDoS attacks and botnets.
- Explain how ethical hackers use DoS or DDoS to assess the damage caused by malicious hackers.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Structure your report as follows:

- Title page.
- Introduction.
- The main body (at least three pages); use headings to identify individual sections.
- Summary and conclusion.

- References page.

Capella academic integrity standards must be strictly followed.

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional
- **References:** Include a minimum of three recent, peer-reviewed references.
- **APA style:** Citations and references must be formatted using current APA style.
- **Length of the report:** A minimum of four typed, double-spaced pages, excluding the title page and references page.
- **Font:** Times New Roman, 12 points.

Course Resources
Journal and Book Locator
Journal and Book Locator Library Guide

u06v1 - Lab: Identifying and Removing Malware on a Windows System

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Identifying and Removing Malware on a Windows System.

Unit 7 >> Social Engineering and Incident Response

Introduction

People are often said to be the weakest link in network security. Attackers attempt to manipulate a user into performing some action, such as clicking on an illicit e-mail link, providing sensitive information, or downloading an attachment. An attacker may also use social engineering techniques in the footprinting stage of their attack. For example, many people reveal information that is useful to attackers on social media. A skilled attacker can leverage this information to increase the effectiveness of an attack. The best firewall will not keep an attacker out of your network if they can trick a user into providing their network credentials. Once a security incident has occurred, compromised credentials for example, it is important to have an incident response plan in place so that the corrective actions are taken contain the threat.

Learning Activities

u07s1 - Studies

Required Readings

Use your *Hacker Techniques, Tools, and Incident Handling* text to read the following:

- Chapter 13, "Social Engineering," pages 313–335.
- Chapter 14, "Incident Response," pages 336–359.

Use the Capella library to read the following:

- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates, and scenarios. *Computers and Security*, *59*, 186–209.
- Kandel, E., & Selarnick, A. (2017). Insuring against social engineering attacks. *Risk Management*, *64*(5), 12, 14.

- Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security*, *73*, 102–113.

Required Skillsoft Videos

For this unit, complete the following:

- Lachance, D. (2017). Security Trends: Identifying social engineering attempts [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CompTIA CASP CS0-003: Reconnaissance, fingerprinting, & social engineering [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Social engineering and phishing [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CISM: Components of an incident response plan [Video]. Skillsoft Ireland.
- Shannon, M. (2016). CISA: Security incident handling and response [Video]. Skillsoft Ireland.
- Shannon, M. (2017). CISM: Techniques to test the incident response plan [Video]. Skillsoft Ireland.
- Hynes, B. (2012). Security essentials: Avoid social engineering attacks [Video]. Skillsoft Ireland.
- Shannon, M. (2017). Security+: Define social engineering and hijacking [Video]. Skillsoft Ireland.
- Welton, T. (2015). IT security for end users: Social engineering scam characteristics [Video]. Skillsoft Ireland.
- Welton, T. (2015). IT security for end users: Avoiding social engineering scams [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional reading from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 10, "Social Engineering."

u07s1 - Learning Components

- Assess how to analyze network traffic to create a baseline definition.
- Practice using key concepts and procedures involved in analyzing network traffic to create a baseline definition.

u07a1 - Analyzing Network Traffic to Create a Baseline Definition

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Analyzing Network Traffic to Create a Baseline Definition lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. Compare and contrast Wireshark and NetWitness.
  2. Explain the steps in the TCP three-way handshake.
  3. List the IP address and protocols types from the Wireshark capture. What Wireshark function can list the different protocols by LAN segment?
  4. Describe the process for determining Wireshark network traffic packet counts.
  5. Describe the relevance of protocol analyzers to information security professionals.
  6. What is baseline analysis?
  7. Compare and contrast internal and external network traffic. What is the relevance of each?
  8. From your lab results, list each protocol and whether it uses TCP or UDP.
  9. What is the difference between TCP and UDP?

Refer to the Analyzing Network Traffic to Create a Baseline Definition scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u07d1 - Social Engineering

Introduction

Social engineering is often utilized by attackers to increase the effectiveness of their attack. Attackers often prey on victims by exploiting emotional responses such as fear, empathy, curiosity, or helpfulness to trick them into performing some action or revealing information. Understanding the techniques used in these attacks is important to mitigation efforts. User training and awareness programs that teach employees how to spot these attacks is a key component of any security program.

Instructions

In a security risk assessment, it was discovered that a malicious insider had convinced employees to reveal confidential company information. The attacker used this information, as well as information found on social media, to target technical support personnel and system administrators. The attacker then sent specially crafted phishing e-mails and eventually tricked a system administrator into installing a malware designed to compromise passwords. The attacker was able to gain access to a privileged account before the exploit was discovered.

For this discussion post, write a report for senior-level management describing the steps you would take to mitigate future social engineering attacks.

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners.

Your initial post should be between 150–200 words and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses should be 75–100 words and are due by 11:59 p.m. CST on Sunday.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u07d2 - Intrusion Detection Systems and Incidence Response

Introduction

Information security incidents are stressful events for security practitioners. Inevitably, you will be faced with responding to an incident at some point in your career. While you may not be able to prevent every incident, creating a plan will assist you in responding appropriately. It is important to create this plan before an incident happens. Documenting lessons learned after an incident is equally important. Naturally, incidents will be stressful but proper planning will allow you to respond correctly.

Instructions

Employees of XYZ Corporation were astonished to discover their network had been hacked. Indicators of compromise (IoC) included known hacking tools, modified file permissions, and multiple connections to an unknown network.

Root cause analysis showed that the attackers had gained access to the network through the demilitarized zone (DMZ) from a compromised web server. A contributing factor in this attack was that the intrusion detection system (IDS) had been misconfigured.

Initiate a discussion describing:

- Concepts, ideas, and thoughts you would include in the incident response plan for this attack.
- A list of testing suites you will use to test your incident response plan.

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners.

Your initial post should be between 150–200 words and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses to other students' posts should be 75–100 words and are due by 11:59 p.m. CST on Sunday.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u07v1 - Lab: Analyzing Network Traffic to Create a Baseline Definition

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Analyzing Network Traffic to Create a Baseline Definition.

Unit 8 >> Defensive Technologies

Introduction

Historically, networks were much more isolated than the contemporary networks we rely on today. Data accessibility has increased exponentially, bringing with it many advantages. However, it has also left organizations more vulnerable to attack. For example, an organization may have their data stored in the cloud instead of on-premises, use extranets to increase productivity, or allow users to work from home using a virtual private network (VPN). This extends the capability of the network but also increases the attack surface. Each connection must be evaluated to understand its overall effect on the security posture of the organization. Organizations must proactively seek to prevent security incidents but must also be ready to detect events when they occur so they can respond appropriately.

Learning Activities

u08s1 - Studies

Required Readings

Use your *Hacker Techniques, Tools, and Incident Handling* text to read the following:

- Chapter 15, "Defensive Technologies," pages 360–385.

Use the Capella library to read:

- Sokol, P., Míšek, J., & Husák, M. (2017). Honeypots and honeynets: Issues of privacy. *EURASIP Journal on Information Security*, *4*, 1–9.

Required Skillsoft Videos

For this unit, complete the following:

- Shannon, M. (2017). CompTIA CASP CS0-003: Host-based IDS and IPS [Video]. Skillsoft Ireland.
- Bigger, D. (2014). CompTIA Network+ 2014: Firewalls and content filters [Video]. Skillsoft Ireland.
- Shannon, M. (2017). Security+: Honeypots [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity Analyst+: Honeypots [Video]. Skillsoft Ireland.
- Lachance, D. (2015). CISSP: Honeypots and honeynets [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional readings from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 15, "Wireless Networking."
- Chapter 16, "Evading IDSs, Firewalls, and Honeypots."

u08s1 - Learning Components

- Analyze how to audit a wireless network and plan for a secure WLAN implementation.
- Practice using key concepts and procedures involved in auditing a wireless network and planning for a secure WLAN implementation.

u08s2 - Assignment Preparation

In the second assignment in Unit 8, Legal Issues and Honeypot Use, you will be asked to write a report for senior management on honeypots and the legal ramifications of using honeypots within an organization. Take time now to review the assignment description and scoring guide.

Then begin preparing for the assignment by researching and analyzing existing IT literature for articles on the following topics:

- Advantages of using honeypots in securing network infrastructures.

- Disadvantages of using honeypots in securing network infrastructures.
- Two types of honeypots and real-life examples.
- Legal ramifications of using honeypots within the organization.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Use the Internet and the Capella University Library Journal and Book Locator for your research.

Use the Journal and Book Locator Library Guide to assist in your research.

u08s2 - Learning Components

- Analyze the advantages of using honeypots in securing network infrastructures.
- Analyze the disadvantages of using honeypots in securing network infrastructures.
- Research at least two types of honeypots.
- Researchy the legal ramifications of using honeypots within the organization.

u08a1 - Auditing a Wireless Network and Planning for a Secure WLAN Implementation

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Auditing a Wireless Network and Planning for a Secure WLAN Implementation lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. Describe the relevance of airmonng, airodump-ng, aircrack-ng, and aireplay-ng in WLAN applications.
  2. Compare and contrast WEP, WPA, and WPA2. Why must wireless network traffic be encrypted?
  3. List some techniques to secure WLAN implementations.
  4. Explain why wireless network security is so important. Is it of equal importance to organizations and home users?
  5. Describe some of the risks, threats, and vulnerabilities associated with wireless networks.
  6. Discuss the risks of using public wireless.
  7. Explain why an organization needs to have a wireless access policy and explain the importance of wireless site surveys.

Refer to the Auditing a Wireless Network and Planning for a Secure WLAN Implementation scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u08a2 - Legal Issues and Honeypot Use

Introduction

In a perfect world, network intrusion prevention measures would be sufficient to prevent any unauthorized network access. Unfortunately, it is impossible to prevent all intrusions. This makes it critical to know when a preventative control has failed. Intrusion detection system and honeypots are two ways an organization can monitor their network for illicit activity. Intrusion detection systems alert an organization to potential illicit activity, while honeypots act as a decoy to lure attackers into an environment where their activities can be closely monitored.

Instructions

Regulations require your organization to perform an annual security assessment, which includes penetration testing. You perform a variety of attacks against the organization's firewall and can breach the network perimeter. In your exploration of the network, you find evidence of a honeypot. Company policy stipulates that only security administrators can implement and manage honeypots. Company policy also explicitly states that all honeypots must be documented and approved by the chief information security officer (CISO).

You report your findings to the CISO, who asks you to provide a report on honeypots and the legal ramifications of using honeypots within the organization.

Write a 3–4 page report in which you:

- Explain the advantages of using honeypots in securing network infrastructures.
- Explain the disadvantages of using honeypots in securing network infrastructures.
- Describe at least two types of honeypots, providing real-life examples.
- Analyze the legal ramifications of using honeypots within the organization.

Your assignment must be supported by a minimum of three recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Structure your report as follows:

- Title page.
- Introduction.
- The main body (at least three pages); use headings to identify individual sections.
- Summary and conclusion.
- References page.

Capella academic integrity standards must be strictly followed.

Assignment Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **References:** Include a minimum of three recent, peer-reviewed references.
- **APA Style:** Citations and references must be formatted using current APA style.
- **Length of the report:** A minimum of three, typed, double-spaced pages, excluding the title page and references page.
- **Font:** Times New Roman, 12 points.

Course Resources
Journal and Book Locator
Journal and Book Locator Library Guide

u08v1 - Lab: Auditing a Wireless Network and Planning for a Secure WLAN Implementation

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

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

Unit 9 >> Investigation Using Linux and Penetration Testing

Introduction

Security professionals proficient in the use of Linux systems will have access to many more security assessment tools than those who are only comfortable using Windows-based systems. For example, the Kali Linux distribution is designed for penetration testing that provides a suite of security assessment tools. Another advantage of Linux is that it can be run off of removable media without requiring installation. It is worthwhile for anyone considering entering the information security profession to become proficient in the use of the Linux operating system.

Learning Activities

u09s1 - Studies

Required Readings

Readings

Use your *Hacker Techniques, Tools, and Incident Handling* to read the following:

- Chapter 12, "Linux and Penetration Testing," pages 300–313.
- Chapter 14, "Incident Response," pages 335–359.
- Chapter 15, "Defensive Technologies," pages 360–385.

Use the Internet to read the following:

- Offensive Security. (n.d.). What is Kali Linux? Retrieved from https://docs.kali.org/introduction/what-is-kali-linux

Required Skillsoft Videos

For this unit, complete the following:

- Lachance, D. (2016). Cybersecurity analyst+: Exploring the Kali Linux suite of tools [Video]. Skillsoft Ireland.
- Lachance, D. (2016). Cybersecurity analyst+: Linux OS monitoring tools [Video]. Skillsoft Ireland.

Optional Resources

Skillsoft Study Guide

The following optional reading from your *CEHv8: Certified Ethical Hacker Version 8 Study Guide* can be used to support your learning in this unit:

- Chapter 16, "Evading IDSs, Firewalls, and Honeypots."

u09s1 - Learning Components

- Examine core concept and principles for assessing and securing systems on a Wide Area Network.
- Practice commands and procedures required to assess and secure systems on a Wide Area Network.

u09s2 - Assignment Preparation

In the second assignment in Unit 9, Incident Response and Intrusion Prevention Strategy, you will be asked to create an incident response and intrusion prevention strategy to address a cyber attack. Take time now to review the assignment description and scoring guide.

Then begin preparing for the assignment by researching and analyzing existing IT literature for articles on the following topics:

- Four guidelines that can be included in a disaster recovery plan to assist in preparing for future attacks.
- Three testing suites that can be used to test a disaster recovery plan.
- Principles and best practices that should be used to handle evidence acquired during the response to an incident.
- Intrusion prevention strategies.

Your assignment must be supported by a minimum of four recent, peer-reviewed references. Citations and references must be formatted using current APA style.

Use the internet and the Capella University Library Journal and Book Locator for your research.

Use the Journal and Book Locator Library Guide to assist in your research.

u09s2 - Learning Components

- Analyze guidelines that can be included in a disaster recovery plan to assist in preparing for future web attacks.
- Analyze Evaluate testing suites that can be used to test a disaster recovery plan.
- Analyze principles and best practices that should be used to handle evidence acquired during the response to an incident.
- Evaluate intrusion prevention strategies.

u09a1 - Investigating and Responding to Security Incidents

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Investigating and Responding to Security Incidents lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.
- Record your answers to the following questions in the same Word document:
  1. At the first indication of comprise, what should you do?
  2. Is malware that is quarantined by an antivirus program considered to be eradicated? Explain your answer.
  3. List the six-step incident handling process recommended by the SANS Institute.
  4. Compare identification and containment during the incident response process.
  5. Should you include the incident response in your information security policy? Explain your answer.
  6. What is the relevance of the post-mortem step during incident response?

Refer to the Investigating and Responding to Security Incidents scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

Course Resources

SANS Reading Room

u09a2 - Incident Response and Intrusion Prevention Strategy

Introduction

To increase business transactions and maximize profits, a health care organization established an international partnership with another health care organization. The appropriate business associate agreements and memorandum of association were put in place. A month after the partnership was initiated, the health care organization was the victim of a cyber-attack. Mitigation efforts were in the millions of dollars.

Instructions

Organizational leadership has requested that you develop a 5–7 page incident response and intrusion prevention strategy.

Your report must:

1. Describe four guidelines that can be included in a disaster recovery plan to assist in preparing for future attacks.
2. Evaluate three testing suites that can be used to test a disaster recovery plan.
3. Describe principles and best practices that should be used to handle evidence acquired during the response to an incident.
4. Describe an intrusion prevention strategy.

Your assignment must be supported by a minimum of four recent peer-reviewed sources. Citations and references must be formatted using current APA style.

Structure your report as follows:

- Title page.
- Introduction.
- The main body (at least five pages); use headings to identify individual sections.
- Summary and conclusion.
- References page.

Capella academic integrity standards must be strictly followed.

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional
- **References:** Include a minimum of four recent, peer-reviewed references.
- **APA Style:** Citations and references must be formatted using current APA style.
- **Length of report:** A minimum of five typed, double-spaced pages, excluding the title page and references page.
- **Font:** Times New Roman, 12 points.

Course Resources
Journal and Book Locator Library Guide
Journal and Book Locator

u09d1 - Linux Tools and Vulnerability Management

Introduction

Kali Linux is an essential tool for anyone involved in penetration testing. Having a good working knowledge of the tools included in the Kali Linux distribution will allow you to investigate and mitigate threats against networks and systems. Another advantage of being proficient using these tools is that you will gain a better understanding of the tools available to attackers.

Instructions

You suspect that hackers have infiltrated your network and launched attacks against many key systems. You need to quickly determine how your systems were compromised.

As a member of the blue team in your organization, discuss:

- Five Kali Linux tool that can be used to assess the attacks.
- How one of the Kali Linux tools can be used to mitigate the attacks.

This discussion will be open-ended to afford you the opportunity to interact with your instructor and other learners.

Your initial post should be between 150–200 words and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

Read the posts of your peers and respond to a minimum of two, expanding on the concepts covered in their initial posts.

Both your initial post and responses to other learners' posts should have a professional tone and be free of grammar and spelling errors. Citations should be formatted using current APA style.

Your responses should be 75–100 words and are due by 11:59 p.m. CST on Sunday.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u09v1 - Lab: Investigating and Responding to Security Incidents

Read the list of questions in this unit's first assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's first assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Investigating and Responding to Security Incidents.

Unit 10 >> IPS, IDS, and Course Reflection

Introduction

During this course, you were introduced to many concepts related to information security. This introduction is a good start, but due to the nature of information security, this is only the beginning. Technology is constantly changing, new threats are emerging, and new methods of defense are being devised. Information is a challenging field, requiring a passion for life-long learning.

Learning Activities

u10s1 - Studies

Required Readings

In your *Hacker Techniques, Tools, and Incident Handling* text, review the following:

- Chapter 14, "Incident Response," pages 335–359.
- Chapter 15, "Defensive Technologies," pages 360–385.

u10s1 - Learning Components

- Analyze how to secure a network with an intrusion detection system.
- Practice using key concepts and procedures involved in securing a network with an intrusion detection system.

u10a1 - Securing the Network with an Intrusion Detection System (IDS)

Instructions

To demonstrate your understanding of core concepts and procedures presented in this unit, you are required to complete the Securing the Network with an Intrusion Detection System (IDS) lab, linked in the courseroom.

As you go through the lab, be sure to:

- Perform all screen captures as the lab instructs and paste them into a Word document.

- Record your answers to the following questions in the same Word document:
  1. Compare IDS and IPS.
  2. What is the significance of obtaining a baseline of network traffic?
  3. Compare host-based IDS and network-based IDS.
  4. Describe some methods to mitigate reconnaissance attacks.
  5. Should host-based IDS be enabled on critical servers and workstations? Explain why or why not.
  6. Discuss where IPS should be placed within the network.

Refer to the Securing the Network with an Intrusion Detection System (IDS) scoring guide to ensure that your work meets the grading criteria for this assignment.

Submit your assignment by midnight Sunday (CST).

Submission Requirements

- **Written communication:** Writing should be clear and well organized, with no technical writing errors, as expected of a business professional.
- **Format:** Typed, double-spaced lines.
- **Font:** Times New Roman, 12 points.

u10d1 - Course Reflections

Instructions

In this final post, reflect on:

1. What you have learned throughout this course.
2. What you have found most interesting in this course.
3. What you have found most challenging in this course.
4. How the skills you have earned in this course will enhance your professional goals.

Your initial post should be between 150–200 words in length and is due by 11:59 p.m. CST on Wednesday of this week.

Response Guidelines

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

Course Resources

Undergraduate Discussion Participation Scoring Guide

u10v1 - Lab: Securing the Network with an Intrusion Detection System (IDS)

Read the list of questions in this unit's assignment before completing this lab. Then record your answers to the questions as you go through the lab.

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

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 will be required to submit the following in this unit's assignment:

- Screen captures from the lab.
- A worksheet with answers to questions about the lab (as listed in the assignment).

Jones & Bartlett Learning Technical Support

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

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

Course Resources

Lab: Securing the Network with an Intrusion Detection System (IDS).