Preview: IAS5100 : Data Engineering

Syllabus

Course Overview

This course engages you in a detailed analysis of the elements of secure data, looking at data structures, databases, software vulnerabilities and data protection used in modern shared data systems. It also provides the opportunity for you to use modern data analysis tools in probing, measuring, and data collection with the goal of identifying and eliminating malware in shared data systems, thus allowing maintenance of their confidentiality, integrity, and availability.

You will also engage in reverse engineering exercises to develop static and dynamic analytical skills for the recovery and maintenance of critical software functionality. The discussions and exercises in this course are structured to engage and develop your skills in critical thinking and analysis to the field of information security.

Please note: The design of this course may be different from that of any other course you have taken at Capella so far. Some of the resources that you need to complete activities can be found in some unit introductions as well as in separate studies. *All* of the resources are valuable and should be considered vital learning materials.

Technology Resources

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

Kaltura Activities

As part of this course, you are required to record video presentations using Kaltura or similar software. Refer to Using Kaltura [PDF] for more information about this courseroom tool.

Disability Services

Note: If you require the use of assistive technology or alternative communication methods to participate in any activity in this course, please contact DisabilityServices@Capella.edu to request accommodations.

Course Competencies

(Read Only)

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

1. Analyze security issues of common data structures and data formats for storing data in a computer system.

2. Apply basic procedures to identify threats and vulnerabilities in software, hardware, and databases.

3. Apply reverse engineering concepts and tools to secure information systems and software.

4. Communicate effectively and professionally.

Course Prerequisites

Prerequisite(s): IAS5130.

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.

Miscellaneous Item

Capella University (Ed.). (2019). *IAS5100: Data engineering* [Custom online lab bundle]. Burlington, MA. Jones & Bartlett. ISBN: 9781284320725.

Custom Reading

These required readings are on the VitalSource platform, available via the VitalSource Bookshelf link in the courseroom, located in your Course Tools.

Capella University (Ed.). (2019). *IAS5100: Data engineering* [Custom text]. Burlington, MA: Jones & Bartlett.

Hardware

Capella University requires learners to meet certain minimum computer requirements. The following hardware may go beyond those minimums and is required to complete learning activities in this course. **Note:** If you already have the following hardware, you do not need to purchase it. Visit the Course Materials page on Campus for more information.

Hardware for Kaltura

Headset with microphone

Broadband Internet connection

Library

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

- Agarkhed, J., & Ashalatha, R. (2017). Security and privacy for data storage service scheme in cloud computing. *International Journal Information Engineering and Electronic Business, 9*(4), 7-12.
- Fanelli, R. (2016). Cyberspace offense and defense. *Journal of Information Warfare, 15*(2), 53–65.
- Kordic, S., Ristic, S., Celikovik, M., Dimitrieski, V., & Lukovic, I. (2017). Reverse engineering of a generic relational database schema into a domain specific data model. Central European Conference on Information and Intelligent Systems.
- Lachance, D. (2014). CompTIA Cloud+: Anti-malware solutions [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Systems security certified practitioner: Malicious code countermeasures [Video]. Skillsoft Ireland.
- Manikandan, G., Rajendiran, P., Harish, V., & Kumar, N. S. (2017). A tree structure based key generation technique for data security enhancement. *Research Journal of Pharmacy and Technology, 10*(9), 2895–2898.
- Nakashima, E. (2018). Pentagon launches first cyber operation to deter Russian interference in midterm elections: Experts are split, however, on how effective the measures will be. *The Washington Post* (online).
- Ramachandran, M. & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management, 36*(4), 618–625.
- Rupprecht, T., Chen, X., White, D., Muhlberg, J., Bos, H., & Luttgen, G. (2016). POSTER: Identifying dynamic data structures in malware. CCS ’16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.
- Slayton, R. (2016). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security, 41*(3), 72–109.
- Stapleton, J. J., & Epstein, W. C. (2016). *Security without obscurity: A guide to PKI operations.* Boca Raton, FL: Auerbach.
- Sun, P, Han, R., Zhang, M., & Zonouz, S. (2016). Trace-free memory data structure forensics via past inference and future speculations. ASCAS ’16 Proceedings of the 32nd Annual Conference on Computer

Security Applications.

- Yongiun, R., Shen, J., Zheng, Y., Wang, J., & Chao, H. (2016). Efficient data integrity auditing for storage security in mobile health cloud. *Peer-to-Peer Network Applications, 9*(5), 854–863.

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.

- Altuwaijri, H. & Ghouzali, S. (2018). Android data storage security: A review. Retrieved from https://www.sciencedirect.com/science/article/pii/S1319157818301046
- Anderson, M. (2018). Tutorial: Introduction to Reverse Engineering. | Transcript Retrieved from https://www.youtube.com/watch?v=7v7UaMsgg_c
- Baruch, R. (2018). Reverse engineering a simple CMOS chip | Transcript Retrieved from https://www.youtube.com/watch?v=FMdYuGpPicw
- CAPEC. (2018) CAPEC-255: Manipulate Data Structures. Retrieved from https://capec.mitre.org/data/definitions/255.html
- Cathyatseneca. (2018). Data structure animations using Processing.js. Retrieved from http://cathyatseneca.github.io/DSAnim/
- Computerphile. (2016). Buffer overflow attack. | Transcript Retrieved from https://www.youtube.com/watch?v=1S0aBV-Waeo Transcript
- cs-Fundamentals.com. (n.d.) Introduction to basic data structures and algorithms. Retrieved from http://cs-fundamentals.com/data-structures/introduction-to-data-structures.php
- CSS Research. (2016). Public key infrastructure for the Internet of Things: White paper. Retrieved from http://cdn2.hubspot.net/hubfs/408597/PKI_for_IoT_White_Paper_CSS_062816.pdf
- Das, A., Da Rolt, J., Ghosh, S., Seys, S., Dupuis, S., Di Natale, G., . . . Verbauwhede, I. (2013). Secure JTAG implementation using Schnorr protocol. *Journal of Electronic Testing, 29*(2), 193–214. Retrieved from http://hal.archives-ouvertes.fr/docs/00/83/79/04/PDF/Secure_JTAG.pdf
- EEVblog. (n.d.). What is JTAG and Boundary Scan? | Transcript Retrieved from https://www.youtube.com/watch?v=TlWlLeC5BUs
- Ellingwood, J. (2014). Understanding the SSH encryption and connection process. Retrieved from https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process
- Evans, J. (2018). How is a binary executable organized? Let’s explore it. Retrieved from https://jvns.ca/blog/2014/09/06/how-to-read-an-executable/
- Gerry_MAN. (2012). What is JTAG? ISP "In-System Programming" JTAG IEEE 1532 Standard (1080p HD). | Transcript Retrieved from https://www.youtube.com/watch?v=Y2j1dEY1zH8
- howCode. (2016). Simple reverse engineering on Windows. | Transcript Retrieved from https://www.youtube.com/watch?v=ZDXTdgfG5HE
- IEEE Standards Association. (2013). IEEE 1149.1-2013 – IEEE standard for test access port and boundary-scan architecture. IEEE Standards Association. (2013). IEEE 1149.1-2013 – IEEE standard for

test access port and boundary-scan architecture. Retrieved from https://standards.ieee.org/standard/1149_1-2013.html

- Ivezic, M. (2018). Stuxnet: The father of cyber-kinetic weapons. Retrieved from https://www.csoonline.com/article/3250248/cyberwarfare/stuxnet-the-father-of-cyber-kinetic-weapons.html
- Kamkar, S. (2018). Getting started with reverse engineering. | Transcript Retrieved from https://www.youtube.com/watch?v=B2MvoBRzrm4
- Kaur, N., & Kaur, P. (2014). Input validation vulnerabilities in web applications. *Journal of Software Engineering, 8*, 116–126.
- Konieczny, T. (2018). Tesla app is insecure by design. This is what Elon Musk can do to change it. Retrieved from https://xsolve.software/blog/tesla-app-insecure-by-design/
- Lin, Z., Zhang, X. & Xu, D. (2010). Automatic reverse engineering of data structures from binary execution. Proceedings of the network and distributed system security symposium, San Diego, CA.
- Mohammadi, A. (2018). How to detect browser exploits and vulnerabilities. | Transcript Retrieved from https://www.youtube.com/watch?v=GAc3kzJZzuE
- NIST. (2013). Special Publication 800-83. Guide to malware incident prevention and handling for desktops and laptops. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final
- NIST. (2018). Dictionary of algorithms and data structures. Retrieved from https://xlinux.nist.gov/dads/
- OWASP. (2016). Testing for SQL injection (OTG-INPVAL-005). Retrieved from https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)
- OWASP. (2017). Input Validation Checklist. Retrieved from https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet
- OWASP. (2018). Input Validation Testing. Retrieved from https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- OWASP. (2018). OWASP Mobile Security Testing Guide. Retrieved from https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
- OWASP. (2018). Reviewing code for cross site scripting. Retrieved from https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting
- OWASP. (2018). Testing for cross site scripting. Retrieved from https://www.owasp.org/index.php/Testing_for_Cross_site_scripting
- Papolu, R. (2018). How to secure your data in the cloud. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/10/11/how-to-secure-your-data-in-the-cloud/
- Patao, I. (2013). Tutorial: Reverse engineering web forms. | Transcript Retrieved from https://www.youtube.com/watch?v=juvgEU9NCxU
- Reiter, R. (2017). Electronics reverse engineering walkthrough – Hacking the Monoprice Select Mini 3D Printer | Transcript Retrieved from https://www.youtube.com/watch?v=T-o-ibGUEoA
- Saleh, H. (2016). Increasing security for cloud computing by steganography in image edges. *Al-Mustansiriyah Journal of Science, 27*(4), 83–85.
- Security Innovation Europe. (2016). What is the difference between hashing and encrypting. Retrieved from https://www.securityinnovationeurope.com/blog/page/whats-the-difference-between-hashing-and-encrypting
- Senrio. (2016) JTAG explained (finally!): Why “IoT”, software security engineers, and manufacturers should care. Retrieved from https://blog.senr.io/blog/jtag-explained
- Smith, J.D. (2015). Reverse engineering your Oracle database to a relational data model. | Transcript Retrieved from https://www.youtube.com/watch?v=hDwJN3KLXWY

- The Web Application Security Consortium. (n.d.) Projects. Retrieved from http://projects.webappsec.org/w/page/13246927/FrontPage
- Toptal. (n.d.). Sorting algorithms animations. Retrieved from https://www.toptal.com/developers/sorting-algorithms
- UC Berkeley. (2018). Database hardening best practices Retrieved from https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/database-hardening-best-practices
- Van den Eijnden, P. (2014). The life-cycle aspect of boundary scan. Retrieved from https://www.evaluationengineering.com/the-life-cycle-aspect-of-boundary-scan.php
- VeraCode. (2018). SQL Injection cheat sheet & tutorial: Vulnerabilities & how to prevent sql injection attacks. Retrieved from https://www.veracode.com/security/sql-injection
- W3Schools. (2018). SQL tutorial Retrieved from https://www.w3schools.com/sql/

Suggested

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

Optional

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

External Resource

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

- Eiman, E. (n.d.). Reversing: Secrets of Reverse Engineering. Retrieved from https://doc.lagout.org/security/Reversing%20Secrets%20of%20Reverse%20Engineering.pdf
- goJTAG. Downloads. Retrieved from http://www.gojtag.com/downloads
- goJTAG. goJTAG - The software. Retrieved from http://www.gojtag.com/package

Unit 1 >> Overview of Data Structures and Algorithms

Introduction

This week you will:

- Examine fundamentals of data structures and algorithms.
- Explore methods for data storage and searches.

A data structure is a specific way to organize data in a computer to optimize the data's use. The goal of data structuring is to reduce both the time complexity of tasks and the space required in memory to store and process data.

Data structures can be linear (such as arrays, linked lists, stacks, and queues), or they can be hierarchical like trees and graphs. In the linear data structures data is arranged in a sequential manner. In the hierarchical structures, data is arranged in a sorted order or in a hierarchical relationship, with relationships formed between parent and child nodes. During runtime of a program, data will be stored, modified, and traversed in different ways depending on the data structure that is used. While data structures define how data is stored, algorithms provide a set of instructions to perform on data such as sorting and searching. How sorts and searches are performed on different data structures will vary.

Learning Activities

u01s1 - Studies

Reading

Read the following in the Capella Library:

- Manikandan, G., Rajendiran, P., Harish, V., & Kumar, N. S. (2017). A tree structure based key generation technique for data security enhancement. *Research Journal of Pharmacy and Technology, 10*(9), 2895–2898.
  - This article explains how a tree data structure is used to improve the generation of private keys to enhance security.

Read the following on the Internet:

- NIST. (2018). Dictionary of algorithms and data structures. Retrieved from https://xlinux.nist.gov/dads/HTML/
  - This site provides a thorough description of the attributes of different data structures and algorithms.
  - Look up and review the information on the following data structures and algorithms.
    - Array.
    - Linked Lists.
    - Stack.
    - Queue.
    - Sort.
    - Search.

        - Hash.

- cs-Fundamentals.com. (n.d.) Introduction to basic data structures and algorithms. Retrieved from http://cs-fundamentals.com/data-structures/introduction-to-data-structures.php
    - This article will introduce you to the basics of data structures and algorithms. This will prepare you for Discussion Topic 1.
- Cathyatseneca. (2018). Data structure animations using Processing.js. Retrieved from http://cathyatseneca.github.io/DSAnim/
    - This website contains animations for common data structures and algorithms. Watch all of the animations to prepare for Discussion Topic 2.
- Toptal. (n.d.). Sorting algorithms animations. Retrieved from https://www.toptal.com/developers/sorting-algorithms
    - This website allows you to view all of the sorting algorithms simultaneously to easily judge which is the fastest. Use the Play All button to watch the sorts occur simultaneously. This will prepare you for Discussion Topic 2.
- Security Innovation Europe. (2016). What is the difference between hashing and encrypting? Retrieved from https://www.securityinnovationeurope.com/blog/page/whats-the-difference-between-hashing-and-encrypting
    - This short article explains the difference between hashing and encryption and will be useful to you in working on this week's lab.

u01s1 - Learning Components

- Understand how a hashed password is created.
- Understand public and private keys.
- Understand how a hashed password is used during login.
- Understand symmetric and asymmetric encryption.

u01s2 - Kaltura Media Preparation

An assignment in this course requires you to record audio for a presentation. You **may choose** to use Kaltura Media or other software. Refer to the Using Kaltura [PDF] tutorial for directions on recording and submitting your recording in the courseroom using Kaltura.

If you have not already done so, set up and test your microphone and headset, using the installation instructions provided by the manufacturer. Then practice using it to ensure the audio quality is sufficient.

Note: If you require the use of assistive technology or alternative communication methods to participate in this activity, please contact DisabilityServices@Capella.edu to request accommodations.

u01d1 - Data Searches

When working with data, there are five fundamental behaviors you are concerned with: access, insert, delete, find, and sort. Different data structures perform these behaviors in different ways, and some data structures do not support all of the behaviors.

Consider the following scenario and assume you:

- Have one product of which you have from 2,000 to 10,000 in stock at any given time.
- Need to keep track of the number of products in stock at any given time.
- Need to be able to say which product came into the warehouse first, so that this product is sold before any others.

Discuss the differences in each of the five behaviors of using ONE of the following.

- Stack.
- Queue.
- Array.
- Binary search.

Justify which method is preferable for the scenario and why it is better than one of the others (your choice, try to pick ones that have been discussed less in the current posts so all methods are covered).

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u01d2 - Data Storage

Select **two** of the scenarios below and discuss which you believe would be the best data structure(s) to fulfill the need presented for your chosen scenarios. There are not necessarily right or wrong answers here, but you must justify your choices.

Scenarios

Imagine you want to digitally store:

- Genealogy information for families.
- Friend networks (i.e. peer to peer relationships) on a social media site.
- Data for the undo and redo functions in word processing software.
- Customer order information for a drive-through fast food restaurant to ensure that customers are charged for correct order at window 1 and that they receive the correct order at window 2.
- Data so that print jobs are printed in the same order they are received.
- Employee passwords at your organization securely.

Data Structure Choices

- Trees.
- Hash Tables.
- Array.
- Linked Lists.
- Stack.
- Queue.
- Dictionary.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

Unit 2 >> Data Structure and Encryption

Introduction

This week you will:

- Apply encryption and hashing algorithms to secure communication in a virtual lab.
- Explore the role of hash table data structure and PKI.

Data structures and algorithms play a role in protecting data both at rest and in transport. This week you will explore the role of the hash table data structure in protecting passwords and protecting data using encryption algorithms that make data unreadable.

These resources focus on cryptography:

- Read the following in your *Hacker Techniques, Tools, and Incident Handling* text:
  - Chapter 3, "Cryptographic Concepts," pages 50–73.
    - This chapter covers cryptography basics used for encryption. You are introduced to symmetrical and asymmetrical encryption as well as hashing and hash tables and how they are used in password protection.
- Ellingwood, J. (2014). Understanding the SSH encryption and connection process. Retrieved from https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process
  - This guide examines the underlying encryption methods used by SSH (secure shell) as well as the connection methods used to establish secure connections. It will help you understand the relationship between encryption and connection methods in forming a connection and authenticating both parties communicating.

Please note: As mentioned at the start of the course, some of the resources that you need to complete activities can be found in unit introductions as well as in separate studies, and the first of these is above. *All* of the resources are valuable and should be considered vital learning materials.

Learning Activities

u02s1 - Studies

Reading

Read the following Internet resource:

- CSS Research. (2016). Public key infrastructure for the Internet of Things: White paper. Retrieved from http://cdn2.hubspot.net/hubfs/408597/PKI_for_IoT_White_Paper_CSS_062816.pdf
    - This article describes how a public key infrastructure can be implemented for the Internet of Things network and devices.

Skillsoft Resources

Read the following in *Security without obscurity: A guide to PKI operations*.

- Chapter 3, "PKI Building Blocks."
    - Introduces building blocks of PKI including architectural elements and selected protocols.
- Chapter 4, "PKI Management and Security."
    - Discusses the management and security of PKI. You will learn what high-level policy statements might be required and goals to be achieved in those policy statements. You will learn the level of detail required in the requirements. You also learn how standards form a bridge between policy and practices.
- Chapter 9, "PKI Governance, Risk, and Compliance."
    - Discusses how an organization must govern PKI systems and the three essential support groups of management, security, and audit. The major roles related to each of the support groups are defined.

u02s1 - Learning Components

- Understand how a hashed password is created.
- Understand how a hashed password is used during login.
- Understand the fundamentals of system user accounts.
- Understand the interconnection of user access and system files.
- Understand symmetric and asymmetric encryption.
- Understand basic data structures and algorithms

u02v1 - JBL Lab: Applying Encryption and Hashing Algorithms for Secure Communication

Overview

Hashing and encryption have two different purposes. A hash algorithm transforms a text string (a file or message) into a fixed-length group of hexadecimal characters. A unique, non-reversible checksum or hash value is produced. The checksum will always be the same unless the file or message content is altered. If the content changes, the hash value or checksum will also change. Hashing allows identification verification for the message sender and also verifies that the content of the message or file has not been altered during transmission. Hashing verifies the integrity of data.

Encryption provides confidentiality of data by changing the message. Once the message or file is changed through encryption algorithms, only someone with the correct and corresponding key can unlock the code and read the original message or file.

Directions

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Section 1, Parts 1-5.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots from Section 1:
    - Part 2: Steps 15, & 19.
    - Part 3: Steps 4 & 6.
    - Part 4: Steps 13 & 21.

Jones & Bartlett Technical Support

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

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

Course Resources

Assignment Template

Jones and Bartlett Lab: Applying Encryption and Hashing Algorithms for Secure Communication

IAS5100: Data Engineering [Custom online lab bundle]

u02a1 - Hashing and Encryption

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

Overview

Information security personnel need to have an in-depth understanding of how to protect the confidentiality and integrity of data. In this assignment, you apply your knowledge of how encryption and hashing protect data against attempts to alter data, read data, or access data without authorization.

Directions

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

Lab Documentation

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

Assignment

1. Imagine that you were able to gain access to a file that held user names and hashed passwords and you also knew the hash function that was used to hash the password, would you then have access to those user accounts? Explain your answer.
2. **Consider the following scenario:** Assume you obtained Alice's Facebook username and password, and Bruce's Facebook password that has the same hash value as Alice's (but a different password). Explain whether or not you will be able to login to Bruce's Facebook account. Example:
    - Alice's password: silo2011.
    - Bruce's password: bob2145sally.
    - Common Hashvalue: 3c9c93e0f8eb2161e5787f7cd3e4b67f8d98fbd80b7d237cc757583b06daa3e3
3. Consider the following scenario: Ann and Bill work for the same company at different remote locations and need to share confidential emails. The IT department in their company naturally wants to ensure the security of these emails so they cannot be intercepted and read by a third party. Do the following:
    - Recommend an encryption procedure and solution that provides an appropriate level of security for their email transactions. Including actions that Ann and Bill need to take to initiate and perpetuate secure communication.
    - Describe the appropriateness of using asymmetric vs. symmetric encryption for this scenario.

Submission Requirements

Submit your Word document with well-labeled responses.

u02d1 - PKI

A public key infrastructure (PKI) is the set of roles, policies, and procedures necessary to create, manage, distribute, use, store, and revoke digital certificates as well as manage public-key encryption.

Select one of the possible applications of PKI below, or describe one of your own.

- Virtual Private Network (VPN).
- A website using Secure Socket Layer (SSL).
- Wireless Authentication.
- Replacing passwords with Smartcards.
- Internet of Things.

Do the following based upon the context chosen above:

1. Describe in detail one of the following key components of Public Key Infrastructure (PKI).
    - Certificate Authority (CA).
    - Registration Authority (RA).
    - Certificate Database.
    - Certificate Store.
2. Discuss the following as they pertain to your application:
    - Why PKI might present a valid security option.
    - The key PKI benefits.
    - The downside (if any) for using PKI.
    - Three to four key phases of implementing a PKI system.
    - What security risks does PKI introduce to the organization and a couple of steps that would mitigate them?

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u02d1 - Learning Components

- Understand public and private keys.

Unit 3 >> Mitigating Data Structure Vulnerabilities and Risks

Introduction

This week you will:

- Perform both static and dynamic quality control testing on a web application in this week's virtual lab.
- Create a presentation on input validation and vulnerability.

Web site and web application security is a high priority. Programmers and web developers have an important role in writing secure code and in understanding the type of testing that is required to ensure that security. This unit explores the Web Application Security Consortium (WASC) - a nonprofit organization that works to improve application security practices. WASC has identified 34 types of web attacks, and 15 web site weaknesses.

Read the following in your *Howto Defend Against Attackers on the Web* text:

- Chapter 6, "Introduction to the Web Application Security Consortium (WASC): The Threats to Web Application Security," pages 148–179.
    - This chapter introduces a wide range of common website attacks. Of particular interest related to data structures will be the sections on buffer overflow, format string, integer overflows, null byte injection, and SQL injection. However, you want to understand all of the threats related to web applications. You will also learn about common website weaknesses, best practices for mitigating web attacks, and best practices for mitigating weaknesses.

Learning Activities

u03s1 - Studies

Reading

Read the following Internet resources:

- Kaur, N., & Kaur, P. (2014). Input validation vulnerabilities in web applications. *Journal of Software Engineering, 8*, 116–126.
    - This journal article describes and discusses the different types of input validation vulnerabilities that can exist on a website.
- CAPEC. (2018). CAPEC-255: Manipulate Data Structures. Retrieved from https://capec.mitre.org/data/definitions/255.html

    - This is the Common Attack Pattern Enumeration and Classification (CAPEC) website. You will be reading about the attack patterns in the Manipulate Data Structures section and will read about mechanisms of these type of attacks. You will then read details about Buffer Manipulation, Shared Data Manipulation, Pointer Manipulation, and Input Data Manipulation. For each attack type, you will see a description, likelihood of attack, severity, relationship to other attack types, prerequisites, consequences, and mitigations.

- OWASP. (2018). Input Validation Checklist. Retrieved from https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet
    - This OWASP checklist aids developers in ensuring they have not overlooked software vulnerabilities due to poor input validation.

- OWASP. (2018). Input Validation Testing. Retrieved from https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
    - This article from OWASP discusses input validation vulnerability testing methods.

- The Web Application Security Consortium. (n.d.) Projects. Retrieved from http://projects.webappsec.org/w/page/13246927/FrontPage
    - Review the projects at the Web Application Security Consortium web page. There are many projects related to different aspects of web application security. Some examples are:
        - Web Security Glossary.
        - Static Analysis Technology Evaluation Criteria.
        - The Web Hacking Incident Database.
    - Anyone can join and become a part of working on any of the listed projects.

- Konieczny, T. (2018). Tesla app is insecure by design. This is what Elon Musk can do to change it. Retrieved from https://xsolve.software/blog/tesla-app-insecure-by-design/
    - Discuss security concerns in Tesla software.

View the following videos on the Internet:

- Computerphile. (2016). Buffer overflow attack. Retrieved from https://www.youtube.com/watch?v=1S0aBV-Waeo | Transcript.
    - Assistant Professor Dr. Mike Pound details how to use a buffer overflow attack to make yourself the Root super-user on a computer running Linux. Also shows disassembling the code.

- Mohammadi, A. (2018). How to detect browser exploits and vulnerabilities. Retrieved from https://www.youtube.com/watch?v=GAc3kzJZzuE | Transcript.
    - This video shows how to use Sploit.IO to detect vulnerabilities and exploits in different web browsers. It compares browsers for security effectiveness.

u03s1 - Learning Components

- Understand secure coding techniques for strong input validation.
- Understand vulnerabilities that exist due to poor input validation.
- Identify the types of attacks that can occur during input validation.

- Identify the types of tests that would reveal input validation vulnerabilities.
- Identify tools that can be used to test for input vulnerabilities.

u03s2 - Kaltura Media

In preparation for creating the audio recordings required for this unit's assignment, do the following **only if you plan to use Kaltura for your presentation**:

- If you have not already done so, set up and test your audio recording device on your computer, using the installation instructions from the manufacturer.
- Practice using the audio equipment to ensure the audio quality is sufficient.
- Refer to the Using Kaltura [PDF] tutorial for directions on recording and uploading your recordings in the courseroom.

Note: If you require the use of assistive technology or alternative communication methods to participate in this activity, please contact DisabilityServices@Capella.edu to request accommodations.

u03v1 - JBL Lab: Performing Dynamic and Static Quality Control Testing (of Software Security)

Overview

Routine vulnerability assessment for web applications helps IT and IT security professionals determine where an attack could potentially occur. There are two types of testing for software applications and web applications: static and dynamic. A common dynamic testing tool is Skipfish. This tool monitors the system as it is operating to detect problems with runtime, performance, and system memory behavior.

Static code analysis, on the other hand, involves analyzing the code for flaws and errors in how it executes. In this lab, you use the Skipfish tool to look for vulnerabilities in the Damn Vulnerable Web Application (DVWA). This is a web application purposely made vulnerable. In addition, you use Rough Auditing Tool for Security (RATS) to perform a static analysis of the code. You view the source code in the vi Editor and then compare the results from the Skipfish and RATS reports.

Directions

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing Section 1, Parts 1 and 2 of the lab.
2. Save the following reports from the lab and submit them with the unit assignment:
    - Section 1, Part 1: Save the Skipfish report as: yourname_S1_skipfish.html
    - Section 1, Part 2: Save the RATS report as: yourname_S1_rats.html

Jones & Bartlett Technical Support

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

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

Course Resources
Jones and Bartlett Lab: Performing Dynamic and Static Quality Control Testing (of Software Security)
IAS5100: Data Engineering [Custom online lab bundle]

u03a1 - Input Validation and Vulnerability Testing Presentation

By now you should have completed the lab in the Virtual Resource Activity for this unit and saved your reports for submission with this assignment.

Overview

Information security personnel need to have a good understanding of secure coding practices for software and web applications and need to understand how to detect flaws in the software and vulnerabilities that exist during program execution. In this assignment you will create a presentation on vulnerability testing and input validation.

Preparation

Follow the steps below to prepare for this assignment.

- Choose a presentation software to create your presentation.
- Consider the following guidelines as you prepare to create your presentation:
    - It is suggested that you write an outline or script of what you are going to say before you begin recording in addition to having your design and supporting visuals ready. Although many software programs allow you to pause or edit, it is advisable to prepare before you start recording.

    - Watch your video prior to posting to ensure that the audio volume is appropriate.

Kaltura

For this assignment, you may choose to create your presentation using Kaltura. To learn how to use Kaltura, refer to the second study in this unit.

Note: If you require the use of assistive technology or alternative communication methods to participate in these activities, please contact DisabilityServices@Capella.edu to request accommodations.

Directions

Lab Documentation

Briefly describe what you learned from or observed in the lab in the *Lab Screenshots and Narrative section* of the Assignment Template found in the Resources. Be specific. **Note:** No screenshots are required for this lab.

Assignment: Presentation on Input Validation and Vulnerability Testing

Prepare and record a 5–7 minute presentation (include voice and supporting visuals) with content and tone appropriate for IT professionals.

Imagine the following scenario:

WidgetWorld is opening a new online portal to sell a variety of bobbles. They have designed an e-commerce application to collect and process typical customer data required to fulfill orders. Naturally, security it a top priority. With e-commerce sites, input validation must be airtight and company risk managers want to be certain of system integrity.

Imagine the company's IT Security Chief has asked you to create a presentation to IT leadership and risk managers that does the following:

- Explains the importance of input validation for security and the consequences of not assuring it.
- Describes **two** insecure coding techniques or errors that leave an application with inadequate input validation.
- Describe two types of tests that should be performed on the e-commerce site to detect the lack of input validation. Explain why they are appropriate.
- Compares their current vulnerability tool (Skipfish) with another tool (of your choosing) that has similar functionality so they can make an informed decision on which to employ going forward. Some things to consider are:
    - Open source vs. proprietary.
    - Reliability.
    - Effectiveness.
    - Application or suitability to the task.
    - Ease of implementation.

Submission Requirements

Submit the following:

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

Course Resources

Assignment Template

u03d1 - Security by Design and Secure Coding

Consult the Internet and your studies to further understand the concept of security by design and how this relates to secure coding practices.

Select one of the attacks listed below that can occur due to lack of secure coding.

- Buffer overflow.
- SQL injection.
- Uncontrolled format string.
- Cross site scripting.

Based on your research, discuss the following:

- An element of insecure coding that allows this type of attack.
- A tool that could be used to detect this vulnerability in the software or website code.
- How this vulnerability can be mitigated through secure coding.
- What might motivate software engineers and software programmers to want to implement secure coding.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u03d1 - Learning Components

- Understand principles of security by design.

Unit 4 >> Introduction to Reverse Engineering

Introduction

This week you will:

- Explore foundational reverse engineering concepts and tools as well as legal issues surrounding reverse engineering.
- Discuss reverse engineering products and tools.

Reverse engineering is a process where the inner workings of an object are extracted. People perform reverse engineering when they are missing knowledge about something like a software program or mechanical object. For example, an organization may have an old database system for which there is no documentation. Reverse engineering would be performed to understand the components and operation of the system so that it could be documented.

Some reverse engineering occurs in order to improve a product's design. Cyber security personnel often reverse engineer code in order to understand how malware operates so that they can develop protections against it.

View the following Internet videos on reverse engineering:

- Anderson, M. (2018). Tutorial: Introduction to Reverse Engineering. Retrieved from https://www.youtube.com/watch?v=7v7UaMsgg_c | Transcript.
  - Mike Anderson of the PTR Group gives a presentation on Reverse Engineering at the Embedded Linux Conference. He explains what reverse engineering is and why it is used. He provides many great examples of reverse engineering. The video is long so you may want to pick and choose which examples you want to watch.
- Kamkar, S. (2018). Getting started with reverse engineering. Retrieved from https://www.youtube.com/watch?v=B2MvoBRzrm4 | Transcript.
  - This is an interview with Samy Kamkar, a security researcher who is well known for using reverse engineering to find a number of vulnerabilities in wireless systems.

Learning Activities

u04s1 - Studies

Videos

View the following Internet videos:

- Patao, I. (2013). Tutorial: Reverse engineering web forms. Retrieved from https://www.youtube.com/watch?v=juvgEU9NCxU | Transcript.
  - This is a short hands-on example of how to reverse engineer a web form.
- howCode. (2016). Simple reverse engineering on Windows. Retrieved from https://www.youtube.com/watch?v=ZDXTdgfG5HE | Transcript.
  - This is a short hands-on video showing how to reverse engineer a Windows.exe file and then manipulate that file.

Optional Resources

- Eiman, E. (2005). Reversing: Secrets of reverse engineering. Retrieved from https://doc.lagout.org/security/Reversing%20Secrets%20of%20Reverse%20Engineering.pdf.

Course Resources

Eiman, E. (n.d.). Reversing: Secrets of Reverse Engineering. Retrieved from https://doc.lagout.org/security/Reversing%20Secrets%20of%20Reverse%20Engineering.pdf

u04s1 - Learning Components

- Understand basics of reverse engineering.
- Identify reverse engineering tools and techniques.

u04d1 - Reverse Engineering Products

Discuss how reverse engineering can be used to examine and understand one of the following:

- Learning tools.
- Features from a software program.
- Designing an aircraft carrier.
- Improving a product.
- Re-creating discontinued parts for an old Mustang using a 3-D printer.

Provide an example of both a legal and illegal use of the reverse engineered product that you chose.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u04d1 - Learning Components

- Understand basics of reverse engineering.

u04d2 - Reverse Engineering Tool Types

Select one of the reverse engineering tool types below and research it on the Internet. Identify at least two tools that perform this function.

- Static Analysis.
- Dynamic Analysis.
- Cryptanalysis.
- Physical Inspection.
- Protocol/Network Interception and Analysis.

Discuss the following:

- The capabilities and features of the two tools that you selected and how they compare.
- Types of vulnerabilities to which you would apply each of those tools.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u04d2 - Learning Components

- Identify reverse engineering tools and techniques.

Unit 5 >> Reverse Engineering of Data Structures

Introduction

This week you will:

- Examine how to reverse engineer both data structures and databases.
- Explore reverse engineering databases.

Data Structures and Databases

Data structures (like arrays, stacks, queues, trees) exist to hold data in a certain structure during runtime of a program. When the program turns off, the data structure and data in it no longer exist. Certain data structures are used in applications to optimize how the data can be retrieved, temporarily stored, and processed when the application is running.

Databases, on the other hand, are external of the application and provide permanent storage for the data. The database is independent of the application but can be accessed by the application. When an application attempts to retrieve customer information from a database the application queries the database for, say, a customer name and address. If the application uses an array data structure, it will place the results of the query into an array data structure and access the data from that data structure while the program is running. Updates to the data (deletions, insertion of new data, update of existing data) might occur while the program is running. Those updates go into the array data structure and then are ultimately written to the database for permanent storage.

Reverse Engineering

As you learned in Unit 4, reverse engineering is a process where you disassemble something to determine how it works. When all you have is a binary executable of a program, you cannot see any of the code or determine what data structures are used. The data structures can be reverse engineered to reveal the underlying semantic and syntactic definitions. This information is needed for many security and forensic applications as it reveals how a program is working.

Databases are reverse engineered to reveal the data model used to design the database. The results are often depicted in an entity relation diagram. This helps to reveal the full picture of how the data is stored, and a full understanding of the data contained in the database, also invaluable for many security and forensic purposes. Reverse engineering often occurs on an executable binary files.

The following resources examine database reverse engineering:

- Kordic, S., Ristic, S., Celikovik, M., Dimitrieski, V., & Lukovic, I. (2017). Reverse engineering of a generic relational database schema into a domain specific data model. *Central European Conference on Information and Intelligent Systems*, 19–28.
    - This article shows how reverse engineering can occur and be used to reverse engineer a generic relational database schema into a domain specific data model.
- Smith, J.D. (2015). Reverse engineering your Oracle database to a relational data model. Retrieved from https://www.youtube.com/watch?v=hDwJN3KLXWY | Transcript.

Learning Activities

u05s1 - Studies

Reading

Read the following Internet resources:

- Evans, J. (2018). How is a binary executable organized? Lets explore it. Retrieved from https://jvns.ca/blog/2014/09/06/how-to-read-an-executable/
    - This article walks through a binary executable file showing how the code is organized.

Optional Reading for Discussion u05d2 (Pick One)

- Rupprecht, T., Chen, X., White, D., Muhlberg, J., Bos, H., & Luttgen, G. (2016). POSTER: Identifying dynamic data structures in malware. *CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1772–1774.
    - Malware grows more complex, necessitating the need to understand the structuring methods used during development. The data structures used by the program are typically not obfuscated. This research exploits that weakness and identifies dynamic data structures present in malware. This aids in reverse engineering and constructing malware signatures, enabling malware classification.
- Sun, P, Han, R., Zhang, M., & Zonouz, S. (2016). Trace-free memory data structure forensics via past inference and future speculations. *ASCAS '16 Proceedings of the 32nd Annual Conference on Computer Security Applications,* 570–582.

  - Reviver solves a problem in forensic analysis which is providing an accurate memory dump data type reverse engineering where any running process within the system can be the target. Reviver constructs the dump's accurate data structure layout by collecting statistical information about possible traces. The program gathers information about past traces, forensic inspection of the current memory dump, and speculation about future executions of suspended processes. From the memory dump, the data structure instances can be inferred.

- Lin, Z., Zhang, X., & Xu, D. (2010). Automatic reverse engineering of data structures from binary execution. Retrieved from https://www.utdallas.edu/~zxl111930/file/Rewards_NDSS10.pdf

u05d1 - Database Documentation

Imagine you are an information security specialist at an organization. The Chief Information Officer (CIO) of the organization has just hired you and explained the following:

- The company uses an onsite database to hold customer information, order information, credit card information, and product inventory information.
- The database was created by the previous database administrator who is no longer employed with the company, and there is no documentation for the database.
- The front-end web site has the web forms that receive input that feeds the database.
- If a customer pulls up their account or order history, the web application queries the database to receive this information.

The CIO wants to document the database, the application code, and how the entire system is structured. Additionally, he wants to assess the security of this entire system.

Discuss the following:

- How you will approach the job and some of the tasks that you must perform.
- The tools that you will use.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u05d2 - Reverse Engineering

Read one of the following and base your discussion upon it.

- Poster: Identifying dynamic data structures in malware.
- Trace-free memory data structure forensics via past inference and future speculations.
- Automatic reverse engineering of data structures from binary execution.

Discuss the following:

1. The primary purpose of the reverse engineering tool or technique for data structures that you read about.
2. The practical application(s) of the tool(s).
3. How the authors will make use of the identified data structures.
4. The conclusions of the authors in the article that you read.
5. Why being able to reverse engineer data structures is so important in forensics.

Make sure to read the response guidelines below, as they differ from other discussions!

Response Guidelines

Identify a student that read a different article than yours. In your response to other students, discuss the similarities and differences in the reverse engineering tool they described and the one that you chose to read about. Discuss whether there were differences in the purpose of the tool, in how the tool was implemented, and in practical applications that were suggested for the tool. In your opinion, which tool has the most valuable practical application and why?

Course Resources

Graduate Discussion Participation Scoring Guide

u05d2 - Learning Components

- Understand basics of reverse engineering.

Unit 6 >> Reverse Engineering and Malware Detection

Introduction

This week you will:

- Identify and remove malware on a Windows system in a virtual lab.
- Explore aspects of malware reverse engineering, protection, and detection.

Malicious software, or malware, describes programs or code that has ill intent and causes harm to systems. The purpose of malware is to take control of a system's operations, usually to damage or shut it down. Malware might retrieve and steal data, encrypt data and then claim a ransom, or delete data. Malware also takes over foundational computer functions and can remain in a system observing computer and network activity undetected.

Sometimes, malware can be detected and removed. However, malware adapts and changes rapidly rendering dated detection and removal tools ineffective. In these instances, one may have to disassemble or dissect the malware to determine how it can be identified and how it works. This is where reverse engineering comes in. By reversing engineering malware code, or the database model, malware analysts can gain the upper hand in this digital game of cat and mouse.

Read the following in your *Hacker Techniques, Tools, and Incident Handling* text for an introduction to malware:

- Chapter 10, "Malware," pages 234–268.

Learning Activities

u06s1 - Studies

Reading

Read the following Internet resource:

- NIST. (2013). Special Publication 800-83. Guide to malware incident prevention and handling for desktops and laptops. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final

Skillsoft Resources

View the following videos:

- Lachance, D. (2014). CompTIA Cloud+: Anti-malware solutions [Video]. Skillsoft Ireland.
- Lachance, D. (2015). Systems security certified practitioner: Malicious code countermeasures [Video]. Skillsoft Ireland.

u06s1 - Learning Components

- Identify reverse engineering tools and techniques.
- Explain principles of static and dynamic analysis.

u06d1 - Ransomware Dilemma

Note: This discussion should be completed before you attempt the unit assignment.

Imagine you are a security analyst that has been contacted by a regional health care provider who has suffered a ransomware attack to their enterprise resource planning (ERP) software server. The company's server is currently paralyzed by the attack and its inoperability has strangled non-patient care operations. Estimates are that this is costing the company anywhere for $25,000 to $200,000 daily. The attackers have demanded $50,000 to restore the system. The company wants to know what they should do.

Discuss what the company should do in order to make an informed decision. Consider the following:

- Questions that should be asked to better understand the situation.
- Important considerations to:
  - Data.
  - Systems.
  - Operations.
  - Privacy.
- Two options that include a brief list of pros and cons.
- Implications or possible outcomes of one of the options.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u06d1 - Learning Components

- Understand basics of reverse engineering.
- Explain principles of static and dynamic analysis.

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

Overview

This lab allows you to use an antivirus tool (AVG) to scan a workstation and view the scan results. You then use AVG's Resident Shield to locate a threat in an archived file that is encrypted. Finally, you will remove the malware that is quarantined in AVG. Finally, you schedule the antivirus scan to run at regular intervals.

Directions

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing section 1, Parts 1–3.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots from Section 1:
    - Part 1: Step 25.
    - Part 2. Step 5.
    - Part 3: Step 3.

Jones & Bartlett Technical Support

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

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

Course Resources

IAS5100: Data Engineering [Custom online lab bundle]

u06a1 - Reverse Engineering and Malware Analysis

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

Preparation

- Search the Internet for a tool(s) or technique(s) that are appropriate for conducting reverse engineering on malware.
- **Note:** Make sure to complete the unit discussion before beginning this assignment.

Directions

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

Lab Documentation

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

Assignment

Consider the scenario presented in the unit discussion. Imagine that the decision has been made to further investigate and attempt to mitigate that attack. You have decided that your approach will be to conduct reverse engineering on the malware to gain a better understanding of how it works. Your job is to explain your approach, in writing, to reverse engineering the malware to the company's IT team and managers.

- Explain what you hope to gain from reverse engineering the malware.
- Describe appropriate static and dynamic analysis tools or techniques that you would use and what they are designed to reveal.

Imagine the following: A co-worker suggested running the malware through a hashing program to help identify the malware. The hash value received using SHA256 is: a24b2b90d11147b3abb916babf95dc007b33dafb

Go to the VICHECK website and enter the hash code. Be sure to open the ViCheck Analysis Details.

- Briefly describe the malware (name, file type, status) and what you learned about it. Consider what you learned and explain how you would use this information as you consider your options for mitigating the attack.

Submission Requirements

Submit a Word document using the format of a professional business letter.

Unit 7 >> Database Specifications and Modification

Introduction

This week you will:

- Explore detecting and mitigating security risks for web servers, databases, and web applications.
- Attack a vulnerable web application and database in a virtual lab.

Security for a commercial website is a complex task. Not only do the web servers have to be protected, but the whole network must be secure. The servers host web pages and web applications, and are typically connected to a database that often contains critical customer and inventory information. This all creates several potential vulnerabilities for websites.

Learn about database attacks in your *Hacker Techniques, Tools, and Incident Handling* text:

- Chapter 9, "Web and Database Attacks," pages 212–232.

Learning Activities

u07s1 - Studies

Reading

Read the following Internet resources:

- UC Berkeley. (2018). Database hardening best practices. Retrieved from https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/database-hardening-best-practices
  - This article presents a thorough review of best practices for hardening a database.
- OWASP. (2016). Testing for SQL injection (OTG-INPVAL-005). Retrieved from https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)
  - This article provides an in-depth evaluation of how to test for SQL injection vulnerabilities.
- W3Schools. (2018). SQL tutorial. Retrieved from https://www.w3schools.com/sql/
  - This is a simple and interactive tutorial to learn the basics of Structured Query Language (SQL).
- VeraCode. (2018). SQL Injection cheat sheet & tutorial: Vulnerabilities & how to prevent SQL injection attacks. Retrieved from https://www.veracode.com/security/sql-injection
  - This is an excellent article that provides code examples for SQL injection and also provides code examples for how to repair code that is vulnerable to SQL injection.

- OWASP. (2018). Testing for cross site scripting. Retrieved from https://www.owasp.org/index.php/Testing_for_Cross_site_scripting
- OWASP. (2018). Reviewing code for cross site scripting. Retrieved from https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting

u07s1 - Learning Components

- Identify the types of SQL Injection that exist.
- Understand coding flaws that allow SQL injection attacks.
- Understand simple SQL commands that can be entered into forms to gain unauthorized access to data in the database.
- Understand Structured Query Language (SQL) is.
- Understand how to repair coding flaws so that vulnerability to SQL injection attacks is removed.
- Identify ways to protect against UNION-based SQL injection attacks.

u07v1 - JBL Lab: Attacking a Vulnerable Web Application and Database

Overview

Regular penetration testing is essential for protecting web applications and web servers and ensuring the confidentiality, integrity, and availability of application, data, or services. In this lab, you use the Damn Vulnerable Web Application, designed with specific vulnerabilities. You act as an ethical hacker hired to help the organization test their web site. To do this, you identify and exploit a cross-site scripting (XSS) vulnerability. You also conduct an SQL injection attack on the SQL database that serves as the backend to the web application. One could do all of this using a browser and simple command strings.

Directions

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

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

1. Follow the lab instructions carefully. **Note:** You are only responsible for completing section 1.
2. Download the Assignment Template found in the Resources and use it for **both your lab screenshots and your assignment responses**.
3. Take the following screenshots from Section 1:
    - Part 2. Step 5.
    - Part 3: Step 19 & 21.
    - Part 4: Step 3.

Jones & Bartlett Technical Support

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

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

Course Resources
IAS5100: Data Engineering [Custom online lab bundle]

u07a1 - Attacking a Vulnerable Web Application and Database

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

Directions

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

Lab Documentation

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

Assignment

Imagine that you have a user's table that contains all of the user IDs and passwords for an organization’s employees. The login form does not have good input validation and will pretty much accept anything that is entered into the form on the login page that asks for userID and password. Do the following:

1. Explain the likely result of entering the following into the userID field on a login screen: "15 OR 1 = 1". Assume that the SQL query that results will be SELECT * FROM Users WHERE userID = 15 OR 1 = 1.
2. Describe actions one could take to protect from this type of SQL injection on the login page of this website.
3. Explain what a UNION-based SQL injection attack is and when one might effectively utilize it to exploit a database.
4. Describe appropriate actions to take to protect from a UNION-based SQL injection attack.

Submission Requirements

Submit a Word document using the format of a professional business letter.

u07d1 - Cross Scripting Vulnerabilities

Imagine that you are the security analyst for an organization that has a web application where users can login and place orders. You have been asked to test the website's security status. As a portion of this test, you want to test for vulnerabilities to cross site scripting (XSS).

Identify two or three cross-site scripting vulnerabilities and the process(s) you would use to test for these vulnerabilities.

Assume that you found an input form on the website that was vulnerable to cross site scripting because fields on the form allow scripts to be entered. Discuss the following:

- How would you approach resolving this problem? Would this vulnerability also allow SQL injection attacks? Explain why or why not.
- What would you include in a training for the organization's web application developers so the risk of cross site scripting and SQL injection attacks would no longer occur?
- Should developers take the approach of checking for incorrect input or check if the input data matches the defined pattern for that field? Justify your response.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u07d1 - Learning Components

- Understand coding flaws that allow SQL injection attacks.
- Understand coding flaws that allow cross site scripting attacks.

- Understand what cross site scripting (XSS) is.
- Understand what SQL injection is.

Unit 8 >> Cloud and Mobile Data Security

Introduction

This week you will:

- Explore data security in the cloud and mobile devices.

This unit explores the concepts of cloud computing, which creates a distributed computing environment that typically involves outsourcing of data storage. The cost and complexity of computing inside the organization sometimes leads to the business decision to outsource some or all aspects of those functions. The material in this unit explore some of the security implications related to the alternatives and choices involved with outsourcing these functions.

Additionally, this unit explores data security in mobile devices such as the security issues that develop with Bring Your Own Device (BYOD) in an organization.

Learning Activities

u08s1 - Studies

Reading

Read the following in the Capella Library:

- Agarkhed, J., & Ashalatha, R. (2017). Security and privacy for data storage service scheme in cloud computing. *International Journal Information Engineering and Electronic Business, 9*(4), 7–12.
    - This article discusses the importance of maintaining security and privacy of data during disaster management and discusses an encryption-based system for data protection while transmitting over the cloud during disaster recovery.
- Ramachandran, M. & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management, 36*(4), 618–625.
    - This research evaluates the performance of recent cloud data security models. They discuss how use of Business Process Model Notation can be effectively used to support data security in the event of a security breach by identifying sections of the security service under attack saving time in data recovery.
- Yongiun, R., Shen, J., Zheng, Y., Wang, J., & Chao, H. (2016). Efficient data integrity auditing for storage security in mobile health cloud. *Peer-to-Peer Network Applications, 9*(5), 854–863.

    - The authors propose a very efficient data integrity auditing process for cloud storage of mobile health applications. Hash operations are used along with encryption during transport of the audit information. The auditing process is greatly sped up.

Read the following Internet resources:

- Altuwaijri, H. & Ghouzali, S. (2018). Android data storage security: A review. Retrieved from https://www.sciencedirect.com/science/article/pii/S1319157818301046
    - This article describes how effective data storage security is on Android devices, and how security on an Android device is implemented.
- Papolu, R. (2018). How to secure your data in the cloud. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/10/11/how-to-secure-your-data-in-the-cloud/
    - This article discusses what individuals and organizations need to do to secure data in the cloud over and above what is the responsibility of the cloud service provider.
- Saleh, H. (2016). Increasing security for cloud computing by steganography in image edges. *Al-Mustansiriyah Journal of Science, 27*(4), 83–85.
    - The authors describe adding the use of steganography as an additional security measure in addition to encryption for security data in the cloud. Steganography is a data hiding method where encrypted data is stored within the edges of color images.
- OWASP. (2018). OWASP Mobile Security Testing Guide. Retrieved from https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
    - This guide provides steps to take in testing security on mobile devices.

u08d1 - Cloud and Mobile Security

As access to mobile-based data becomes increasingly prevalent, it is a matter of growing importance that data engineering techniques become more sophisticated in meeting a growing range of threats, both internal and external to the data systems involved.

Discuss the following as they pertain to smart phone security:

- How concerned are you about the security risks on your personal smartphone? What security risk is your biggest concern and why?
- Discuss three of the following with regard to Apple iOS, Windows, or Android.
    - What is required to maximize security on your smartphone.
    - Security options that would hinder performance that you might choose not to use. If you choose to disable, what would be the security risk?

- Security features that are built into the smartphone by the manufacturer and ones that are settings that you can manipulate.
- Your confidence that when security settings are correctly set, that your privacy and data are secure.
- Describe additional security features you would like to see implemented in smartphones.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u08d2 - Important Lessons Learned

This course is focused on the critical competencies necessary to thoroughly understand the challenges facing contemporary information security and the tools and techniques that are evolving to meet those needs. Data engineering is a multi-faceted topic. To focus only on unique aspects of the field is dangerous. A holistic approach must be taken in providing data confidentiality, integrity, and availability in the increasingly virtual environment.

Now it is time to pause and discuss two or three of the most important lessons you have learned so far in this course so far. Importantly, analyze how they relate to one another.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

Unit 9 » Analysis and Implication of JTAG Standards

Introduction

This week you will:

- Explore the JTAG standard (IEEE 1149.1).
- Explain aspects of a JTAG implementation.
- Apply JTAG in an optional lab.

Joint test action group (JTAG) is the name most commonly referred to when discussing the IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture. Unit 9 covers this standard, which is designed for system debugging.

JTAG is a basic hardware interface that gives your computer or embedded devices the ability to communicate directly with the circuit board chips. Today JTAG is used for programming, debugging and testing all embedded devices. The high density of integrated circuits caused a need to be able to test the physical interconnections, but the density of the circuit boards made it impossible to insert probes. JTAG provided the solution.

In addition to testing connections, JTAG, by giving direct access to devices, is a good tool for security research. However, JTAG poses its own security risks because it does give such easy access to the hardware integrated circuits. The potential security impact of getting JTAG access to a device is huge. Having that access allows you to see data movement, modify data, dump RAM contents and FLASH chips on the circuit board. On a positive note, this type of access also allows software debugging through hardware.

JTAG is present on almost every embedded device, making those devices very vulnerable. Protecting against attacks on embedded devices requires that the embedded devices be monitored.

Learn more about JTAG by reading the following:

- IEEE Standards Association. (2013). IEEE 1149.1-2013 – IEEE standard for test access port and boundary-scan architecture. Retrieved from https://standards.ieee.org/standard/1149_1-2013.html
  - This describes the IEEE 1149.1-2013 JTAG standard, providing details of the standard, additional resources about the standard, and working group information.

Course Resources

IEEE 1149.1-2013 – IEEE standard for test access port and boundary-scan architecture.

Learning Activities

u09s1 - Studies

Reading

Read the following Internet resources:

- Senrio. (2016). JTAG explained (finally!): Why "IoT", software security engineers, and manufacturers should care. Retrieved from https://blog.senr.io/blog/jtag-explained
  - This article explains what JTAG is, why manufacturers use JTAG, core elements of JTAG, what JTAG is not, and the five required JTAG signals. A good example of how JTAG would be used is provided.
- Van den Eijnden, P. (2014). The life-cycle aspect of boundary scan. Retrieved from https://www.evaluationengineering.com/the-life-cycle-aspect-of-boundary-scan.php
  - This article discusses how JTAG can be implemented across the phases of the product life cycle.
- Das, A., Da Rolt, J., Ghosh, S., Seys, S., Dupuis, S., Di Natale, G., . . . Verbauwhede, I. (2013). Secure JTAG implementation using Schnorr protocol. Journal of Electronic Testing, 29(2), 193–214. Retrieved from http://hal.archives-ouvertes.fr/docs/00/83/79/04/PDF/Secure_JTAG.pdf

Video

View the following Internet Videos:

- EEVblog. (n.d.). What is JTAG and Boundary Scan? Retrieved from https://www.youtube.com/watch?v=TlWlLeC5BUs | Transcript.
- Gerry_MAN. (2012). What is JTAG? ISP "In-System Programming" JTAG IEEE 1532 Standard (1080p HD). Retrieved from https://www.youtube.com/watch?v=Y2j1dEY1zH8 | Transcript.

u09s1 - Learning Components

- Explain fundamental principles of JTAG.
- Understand basics of reverse engineering.
- Identify components of the product life cycle.
- Identify the uses and limitations of JTAG in product development.
- Understand how JTAG is applied to product development.
- Understand the security risks related to JTAG.

u09a1 - Applying IEEE 1149.1 (JTAG)

Overview

JTAG has evolved considerably since its original standard in 1990, which was the boundary scan specification. In 2002, in-system configuration or programmable devices was added to the standard. In 2012, stimulus of interconnects to passive and active components was added. In 2014, access and control of embedded instruments within a semiconductor device was added. Currently, JTAG tools are used in all phases of the product life cycle. Since 1990, this standard has been used by electronics companies all around the globe. JTAG's original use was to test for faults in integrated circuits that were being made in a way that connections between integrated circuits were not accessible by probes. The standard essentially provided a pins-out view from one IC pad to the other.

Over the years, the application of JTAG has expanded to many other areas. It is now used for whole system testing, fault detection, and diagnosis by accessing sub-blocks of integrated circuits. It can also debug software in embedded systems. JTAG is also used to store firmware in devices. It allows the detection of both software and hardware defects and an operating computer or system can be monitored.

JTAG is basically an interface that is added to a chip. and it can facilitate daisy chaining multiple chips. Today, almost all embedded systems have a JTAG port to facilitate in-circuit debugging and firmware programming.

Preparation

Select one of the phases listed below and perform Internet research for an example of a product that uses JTAG to implement that phase of the product life cycle.

- Design.
- Hardware Debug.
- Software Debug.
- Integration and Testing.
- Production.
- Maintenance and Service.

Directions

- Describe in detail how JTAG was implemented in your chosen example.
- Explain the benefits and limitations of using JTAG at this phase of the product development life cycle.
- Discuss the security risks that emerge as JTAG is implemented on a device.
- Another common use for JTAG is reverse engineering. Describe how you might use JTAG to reverse engineer the product.

Submission Requirements

Submit a 2–3 page double spaced Word document with well-labeled responses.

u09d1 - IEEE 1149.1 (JTAG) Standard

The IEEE 1149.1 (JTAG) standard provides a common and useful technique for data systems development, debugging, and testing. When evaluating JTAG, it is critical to consider the management issues involved, such as cost, complexity, and susceptibility of JTAG test beds to exploitation by hackers desiring to mount cryptographic attacks.

Discuss an instance where a key management problem has been overcome in the successful implementation of IEEE 1149.1 using public-key cryptography. Include in your discussion the effects of the said technique on JTAG implementation overhead cost.

Make sure to cite your sources.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u09d1 - Learning Components

- Explain fundamental principles of JTAG.

u09s2 - JTAG Lab (optional)

This optional exercise provides hands-on experience with JTAG.

goJTAG software is a university-driven open source product from Tallinn University of Technology and allows you to study boundary-scan techniques, to run diagnosis tests, and run your own experiments. The software comes with a built-in demo project. The software allows you to inject faults (like short circuits) and look at boundary scan results. goJTAG is available for Windows and Linux operating systems.

You can download the software here: http://www.gojtag.com/downloads

After it is downloaded, install the software. It installs very quickly and will open when the install finishes.

Then go to this link for a Quick Start Guide to open a sample project and run your first scan: http://www.gojtag.com/package

Course Resources

goJTAG. Downloads. Retrieved from http://www.gojtag.com/downloads

goJTAG. goJTAG - The software. Retrieved from http://www.gojtag.com/package

Unit 10 >> Cyber Ops

Introduction

This week you will:

- Explore cyber-operations tools, phases, and techniques.
- Discuss aspects of Stuxnet cyber-weapon.

"Cyber-operations" is a relatively new concept. Though there have been many examples of cyber-operations through the past few decades, the Stuxnet operation was likely the most visible and had the highest impact. This unit explores cyber-operations, the phases of a cyber-operation, and the roles involved with cyber-operations. Studies cover both cyber-operations from a defensive and offensive perspective.

Learning Activities

u10s1 - Studies

Reading

Read the following In the Capella library:

- Nakashima, E. (2018). Pentagon launches first cyber operation to deter Russian interference in midterm elections: Experts are split, however, on how effective the measures will be. *The Washington Post* (online).
  - This article talks about tactics the United States is using to deter Russian operatives from interfering in our recent midterm election.
- Fanelli, R. (2016). Cyberspace offense and defense. *Journal of Information Warfare, 15*(2), 53–65.
  - This article discusses how standard military operations somewhat apply in cyber warfare and discusses this in depth. The author takes a more technological view of cyberspace defense and offence, comparing this to the traditional military concepts.
- Slayton, R. (2016). What is the cyber offense – defense balance? Conceptions, causes, and assessment. *International Security, 41*(3), 72–109.
  - This article discusses how organizational skills and technologies must be included in any discussion about balancing offense and defense. The author defines balance in dyadic terms – the value less the costs of offensive operations and the value less the costs of defensive operations.

Internet Resources

- Ivezic, M. (2018). Stuxnet: The father of cyber-kinetic weapons. *CSO.* Retrieved from https://www.csoonline.com/article/3250248/cyberwarfare/stuxnet-the-father-of-cyber-kinetic-weapons.html
  - This article describes how Stuxnet works and its beginnings. The article also discusses continuing threats.

Videos

- Reiter, R. (2017). Electronics reverse engineering walkthrough – Hacking the Monoprice Select Mini 3D Printer. Retrieved from https://www.youtube.com/watch?v=T-o-ibGUEoA | Transcript.
  - This video provides an introduction to how to approach reverse engineering of hardware.
- Baruch, R. (2018). Reverse engineering a simple CMOS chip. Retrieved from https://www.youtube.com/watch?v=FMdYuGpPicw | Transcript
  - This video shows reverse engineering a National Semiconductor 54HC00 quad NAND gate.

u10d1 - Stuxnet Cyberwarfare

The Stuxnet attack is arguably the most famous incident of what has been termed "cyberwarfare." Its basis, design, and impact continue to form a major justification for the development of robust countering strategies and tools which can inhibit the effects of malware employed in strategic roles. Yet, the attack was possible because of design characteristics of the technology employed by Iran in its nuclear centrifuge program. This question focuses on that design.

Perform research on the internet and analyze, then discuss the engineering vulnerabilities inherent in the Siemens S7-417 controller that allowed the Stuxnet attack to occur. Briefly describe the impact of the attack on the IT Security community.

Include in the discussion the ethical and legal implications of countries engaging in this type of cyberwarfare against one another.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.

Course Resources

Graduate Discussion Participation Scoring Guide

u10d2 - Defensive Cyber Ops: Phases, Tools and Techniques

You have been exploring cyber-operations from an offensive position. In keeping with the idea that for every offensive action there is a corresponding need for a defensive position.

Use the Internet and resources in this unit's studies to discuss the phases, tools, and techniques that make up a cyber-operation from a defensive perspective. Include in the discussion the IT security roles that should be responsible for ensuring the success of this defensive action.

Response Guidelines

As with most discussions in this course, it is recommended that you post your initial post early to allow time for your peers to respond. Read the posts of at least two of your peers and provide feedback.

The minimum expectation within course discussions is to respond to at least two posts at the earliest, but it is highly recommended that you extend the dialogue further. Responding over multiple days will help in stimulating a lively discussion. Provide responses to your peers early if possible so that you will have more opportunity for an in-depth interaction with your peers and the instructor.