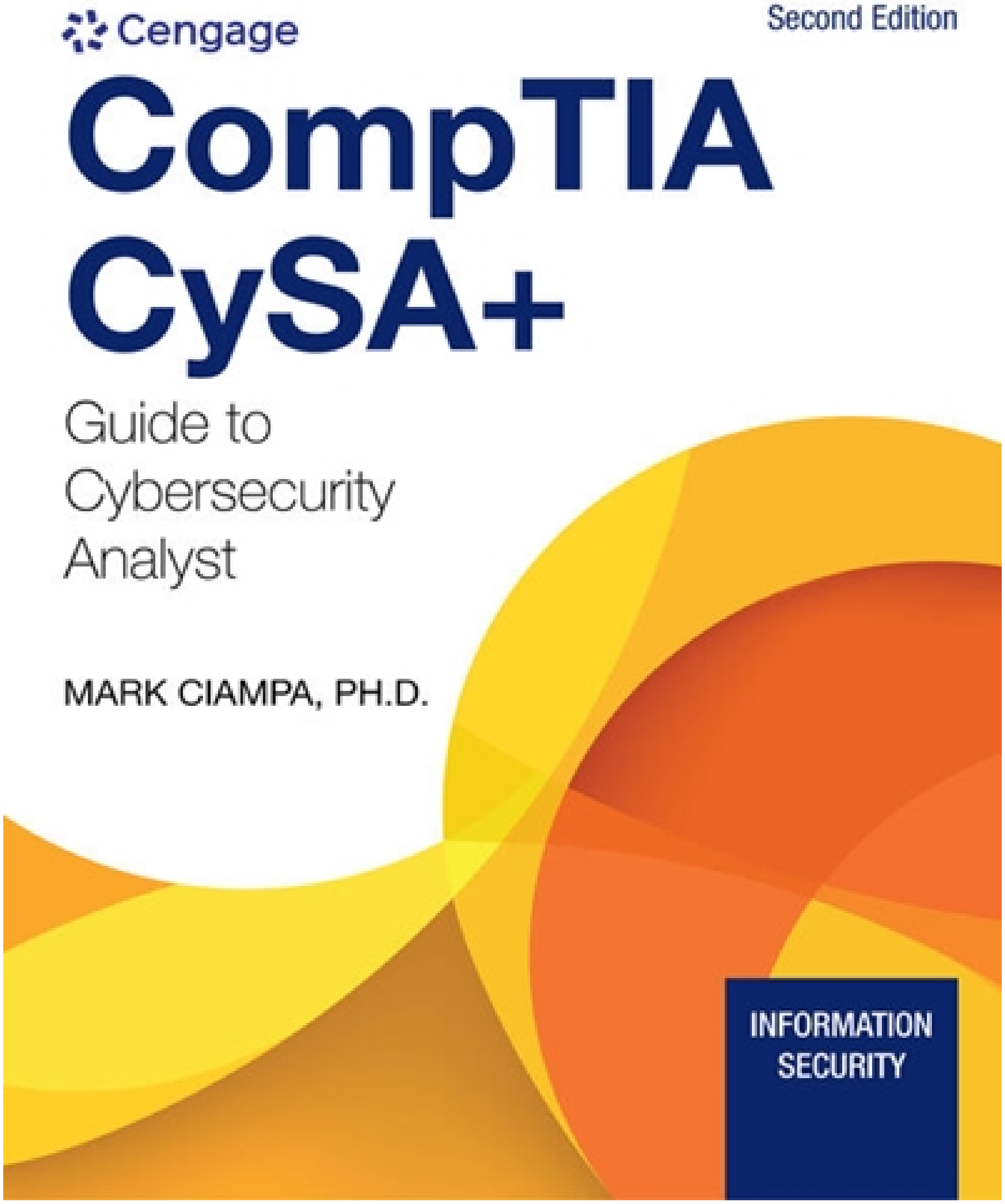
Solutions for CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd Edition by Ciampa



Cengage

Second Edition

CompTIA CySA+

Guide to Cybersecurity Analyst

MARK CIAMPA, PH.D.

INFORMATION SECURITY

Solutions

Solution and Answer Guide

Mark Ciampa, CompTIA CySA+ Guide to Cybersecurity Analyst, 2nd Edition, ISBN: 9780357677995; Module 01: Enterprise Threats and Vulnerabilities

Table of Contents

Review Questions

1. Which of the following is FALSE about rootkits?

   a. A rootkit is malware that can hide the presence of other malware.

   b. Rootkits continue to be used extensively and their usage has not diminished.

   c. Rootkits can be used to hide its own presence.

   d. Rootkits cannot be detected by either an OS or common antimalware scanning software.

Answer: b. Rootkits continue to be used extensively and their usage has not diminished.

Explanation: The risks of rootkits in OSs are significantly diminished today due to protections built into modern OS software. These protections include preventing unauthorized kernel drivers from loading, stopping modifications to certain kernel areas used by rootkits to hide, and preventing rootkits from modifying the bootloader program.

2. What is the goal of a buffer overflow attack?

a. To change the address in the buffer to the attacker's malware code

b. To cause the computer to function erratically

c. To steal data stored in RAM

d. To link to an existing rootkit

Answer: a. To change the address in the buffer to the attacker's malware code

Explanation: A buffer overflow attack occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer, and this extra data overflows into the adjacent memory locations. Because the storage buffer typically contains the "return address," an attacker can overflow the buffer with a new address pointing to the attacker's malware code.

3. Which area of computer memory is dynamic memory for the programmer to allocate as necessary?

a. Text

b. Stack

c. Heap

d. Data

Answer: c. Heap

Explanation: The heap is dynamic memory for the programmer to allocate as necessary.

4. Jan is explaining to his colleague the reasons why a web application infrastructure is a tempting target for attackers. Which of the following is NOT a reason Jan would give?

a. A successful compromise could impact all web users who access the web server.

b. An attack could provide a pathway into the enterprise's network infrastructure.

c. An attack on a web application infrastructure is considered the easiest attack to create.

d. The multiple elements in a web application infrastructure provide for a range of vulnerabilities that can be used as different attack vectors.

Answer: c. An attack on a web application infrastructure is considered the easiest attack to create.

Explanation: A web application attack is not the easiest attack to create.

5. Which of the following is FALSE about a cross-site scripting (XSS) attack?

a. The underlying web application that accepts the malicious code becomes the vehicle to deliver the malicious script to every user's browser when he or she accesses that site.

b. An attacker attempts to execute malicious scripts in the victim's web browser by directly injecting it into the user's web browser.

c. XSS is essentially a client-side code injection attack using a web application.

d. The term cross-site scripting refers to an attack using scripting that originates on one site (the web server) to impact another site (the user's computer).

Answer: b. An attacker attempts to execute malicious scripts in the victim's web browser by directly injecting it into the user's web browser.

Explanation: An attacker attempts to execute malicious scripts in the victim's web browser but not by directly injecting it into the user's web browser. Rather, the attacker inputs that malicious code on a website that accepts user input. The underlying web application that accepts the malicious code then becomes the vehicle to deliver the malicious script to every user's browser when they access that site.

6. Ricardo is reviewing the different types of XSS attacks. Which attack only impacts the user who entered the text on the website?

a. Reflected XSS

b. Persistent XSS

c. Document Object Model XSS

d. Universal XSS

Answer: a. Reflected XSS

Explanation: In a Reflected XSS attack, the user enters input into a web application that is then immediately displayed back ("reflected") to that user to initiate the attack.

7. What is the goal of a SQL injection attack?

a. To corrupt data in the database

b. To manipulate a NoSQL database

c. To extract data from a database

d. To inject malware that will infect the web browsers of subsequent users

Answer: c. To extract data from a database

Explanation: The goal of a SQL injection attack is to exfiltrate data from a SQL database.

8. Bette is researching how a session hijacking attack could occur. Which of the following would she NOT find as a means for the attack to occur?

a. MITM

b. XSS

c. Guessing the session ID

d. MVFL

Answer: d. MVFL

Explanation: This is fictitious and does not exist.

9. Which of the following is FALSE about a password spraying attack?

a. It takes one or a small number of commonly used passwords in attempts to break into an account.

b. Because it is spread across many different accounts, it is much less likely to raise any alarms.

c. It is considered as the optimal means for breaking into accounts.

d. It is a type of targeted guessing.

Answer: c. It is considered as the optimal means for breaking into accounts.

Explanation: Although password spraying may result in occasional success, it is not considered the optimal means for breaking into accounts.

10. Why is credential stuffing effective?

    a. Because users repeat their passwords on multiple accounts

    b. Because it can circumvent all known password security protections

    c. Because it is the fastest known password cracking attack

    d. Because it is the oldest and most reliable attack on passwords

Answer: a. Because users repeat their passwords on multiple accounts

Explanation: Because users repeat their passwords on multiple accounts, attackers use these passwords in their attacks with a high probability of success and this is known as credential stuffing.

11. What is the goal of a directory traversal attack?

    a. It has no goal other than to silently look through files stored on a file server.

    b. Its goal is to move from the root directory to other restricted directories.

    c. Its goal is to identify a vulnerability in a server or endpoint so that access can be gained into a network.

    d. Its goal is to pivot to another server.

Answer: b. Its goal is to move from the root directory to other restricted directories.

Explanation: Threat actors may use a directory traversal attack that takes advantage of a vulnerability in a web application or web server software so that a user can move from the root directory to other restricted directories.

12. What is pretexting?

    a. Sending text messages to selected victims

    b. Obtaining private information

    c. Preparing to enter a network through a RCE vulnerability

    d. Moving laterally before entering a vulnerable endpoint

Answer: b. Obtaining private information

Explanation: Sometimes the goal of impersonation is to obtain private information, known as pretexting.

13. Which type of OS is found on an embedded system?

a. RSTS

b. SoC

c. RTOS

d. XRXS

Answer: c. RTOS

Explanation: A real-time operating system (RTOS) is a specifically designed OS for an SoC in an embedded or specialized system.

14. Aiko has been asked by her friend if she should download and install an app that allows her to circumvent the built-in limitations on her Android smartphone. What is this called?

a. Jailbreaking

b. Side-caring

c. Rooting

d. Pivoting

Answer: c. Rooting

Explanation: Users can circumvent the installed built-in limitations on their smartphone, which is called rooting on Android devices.

15. Aiya wants a new notebook computer. She has asked a technician about a model that has USB OTG. Which of the following would the technician NOT tell Aiya about USB OTG?

a. A device connected via USB OTG can function as a peripheral for external media access.

b. A device connected via USB OTG can function as a host.

c. Connecting a mobile device to an infected computer using USB OTG could allow malware to be sent to that device.

d. USB OTG is only available for connecting Android devices to a subnotebook.

Answer: d. USB OTG is only available for connecting Android devices to a subnotebook.

Explanation: USB OTG is available for a wide range of devices and not just Android.

16. The organization for which Cho works has just purchased a manufacturing plant that has many machines using Modbus. Cho has been asked to research Modbus. Which of the following will Cho NOT find regarding Modbus?

a. Many SCADA systems use Modbus.

b. The original version of Modbus used serial ports.

c. A later variation to Modbus incorporated the TCP/IP protocol.

d. Modbus is robust security.

Answer: d. Modbus is robust security.

Explanation: Although standard Modbus has error-detection capabilities to protect against data corruption, it has no security protections against injected commands or the interception of data.

17. What is the network used in vehicles for communications?

a. CAN

b. ECU

c. EDU

d. M-BUS

Answer: a. CAN

Explanation: The controller area network (CAN) bus network is used for sending and receiving data in vehicles.

18. Which of the following is NOT a security constraint for embedded systems and specialized devices?

a. Power

b. Compute

c. Cost

d. Patches

Answer: d. Patches

Explanation: Patches are not a constraint but are “fixes” to vulnerabilities.

19. Which of the following is the greatest asset but also a security vulnerability of a mobile device?

a. Low cost

b. Portability

c. Cameras

d. Small screen

Answer: b. Portability

Explanation: The greatest asset of a mobile device—its portability—is also one of its greatest vulnerabilities. Mobile devices are frequently lost or stolen because, by their very nature, they are designed for use in a wide variety of locations, both public (coffee shops, hotels, and conference centers) and private (employee homes and cars). These locations are outside of the enterprise's normal protected physical perimeter of walls, security guards, and locked doors.

20. What is geo-tagging?

a. Restricting where an app functions based on its location.

b. Adding geographical identification data to media.

c. Tracking a victim who is wearing a GPS-enabled wearable device.

d. Using the GPS feature of a smartphone.

Answer: b. Adding geographical identification data to media.

Explanation: A related risk is GPS tagging or geo-tagging, which is adding geographical identification data to media such as digital photos taken on a mobile device. A user who, for example, posts a photo on a social networking site may inadvertently identify a private location to anyone who can access the photo.

Case Projects

Case Project 1-1 Rootkits

Research how rootkits can evade detection from an OS or antimalware software. What techniques does it use to hide itself? How can it hide other malware? Besides hiding malware on a hard drive, where are other locations that rootkits can hide malware? Write a one-page paper on your research.

Answer: Rootkits are considered unique among malware variants, as they are created and distributed with the intention of hiding. There are three main kinds of rootkits: kernel, hardware/firmware, and bootloader. There are other types of rootkits as well, such as hypervisor/virtual, user-mode, and memory variants, but these are less common. The most common and most complex types of rootkits are kernel rootkits that function at the OS level and can change the way the OS works. Kernel rootkits may add their own code into the OS kernel or can delete and replace code. Hardware or firmware rootkits hide inside hardware or in system firmware. They can actually have some legitimate uses, such as in anti-theft programs that can help find stolen devices. The final type is a bootloader rootkit that can target the hard drive's master boot record. They replace or change the real bootloader with their own, giving them control over the operating system. This allows the bootloader rootkit to activate the boot kit before the OS starts.

Although rootkits are difficult to detect, some techniques used to find a rootkit include:

- Boot a computer as a "known clean machine" and then use runtime tools to look for rootkit components.
- Look for alerts to unusual traffic.
- Run a rootkit scan.
- Use a behavioral analysis tool to look for anomalous behaviors and behaviors commonly displayed by rootkits.
- Use machine learning static analysis for rootkit detection.

Case Project 1-2 Heap Overflow

Research heap overflows. How do they work? How can they be prevented? How common is this type of attack? Write a one-page paper on your research. Include a drawing of how RAM looks before and after a heap overflow attack.

Answer: A heap overflow is a form of buffer overflow; it happens when a chunk of memory is allocated to the heap and data is written to this memory without any bound checking being done on the data. This is can lead to overwriting some critical data structures in the heap such as the heap headers, or any heap-based data such as dynamic object pointers, which in turn can lead to overwriting the virtual function table. Much like a stack buffer overflow, a heap overflow is a vulnerability where more data than can fit in the allocated buffer is read in. This could lead to heap metadata corruption, or corruption of other heap objects, which could in turn provide new attack surface.

In the event that an unsafe function leaves an open overflow opportunity this could result in a vulnerability for a threat actor to exploit a heap overflow. Advances are being made to help detect these vulnerabilities at compile and runtime. When running a program, compilers often create random values known as "canaries" and place them on the stack after each buffer. Much like the coalmine birds for which they are named, these canary values can flag a dangerous situation. Checking the value of the canary against its original value can determine whether a buffer overflow has occurred. If the value has been modified, the program can be shut down or go into an error state rather than continuing to the potentially modified return address. Additional defenses are provided by some of today's operating systems in the form of non-executable stacks and address space layout randomization (ASLR). Non-executable stacks (i.e., data execution prevention [DEP]) mark the stack and in some cases other structures as areas where code cannot be executed. This means that an attacker cannot inject exploit code onto the stack and expect it to successfully run.

Case Project 1-3 Document Object Model XSS

Search the Internet for information on Document Object Model XSS. What is a Document Object Model (DOM)? Where are they found? How do threat attacks attempt to compromise them? How can they be used in an XSS attack? What is the defense against them? Write a one-page paper on your research.

Answer: The Document Object Model (DOM) is the data representation of the objects that comprise the structure and content of a document on the web. DOM is a programming interface for HTML and XML documents. It represents the page so that programs can change the document structure, style, and content. The DOM represents the document as nodes and objects. This permits programming languages to connect to a web page. That means the DOM represents that same document so it can be manipulated. In short, the DOM is an object-oriented representation of the web page, which can be modified with a scripting language such as JavaScript.

There are standards for DOM implemented in most modern browsers, and many browsers extend the standard, so that care must be exercised when using them on the web where documents may be accessed by various browsers with different DOMs. The modern DOM is built using multiple APIs that work together. The core DOM defines the objects that fundamentally describe a document and the objects within it. This is expanded upon as needed by other APIs that add new features and capabilities to the DOM. For example, the HTML DOM API adds support for representing HTML documents to the core DOM.

A DOM XSS is a cross-site scripting vulnerability that appears in the DOM instead of part of the HTML. In reflective and stored XSS scripting attacks you can see the vulnerability payload in the response page. In a DOM XSS the HTML source code and response of the attack will be exactly the same so the payload cannot be found in the response. Rather, it can only be observed on runtime or by investigating the DOM of the page.

The primary defense against a DOM XSS is that untrusted data should only be treated as displayable text. This means developers should avoid treating untrusted data as code or markup within JavaScript code.

Case Project 1-4 Real-Time Operating System (RTOS)

What features are found in a real-time operating system? How is it specifically designed for a SoC? What are its advantages? What are its disadvantages? Compare the features of three RTOSes and create a table listing each along with its features. Write a one-page paper on your research.

Answer:

Features of RTOS:

- Consume fewer resources.
- Occupy less RAM.
- Response times are highly predictable.
- The kernel restores the state of the task and passes control of the CPU for that task.
- The kernel saves the state of the interrupted task ad then determines which task it should run next.

Disadvantages of RTOS:

- It uses complex algorithms that can be difficult to understand.
- Many resources are used by RTOS, which can make the system expensive.
- RTOS concentrates on a few task, making it difficult to perform multi-tasking.
- Specific drivers are required for the RTOS so that it can offer fast response time to interrupt signals.
- The tasks which have a low priority need to wait for long periods of time as the RTOS maintains the accuracy of the program, which are under execution.

A comparison of features depends on which RTOSes are chosen.

Case Project 1-5 On the Job

Suppose you work for a company that has just hired a new senior vice president. After reviewing the budgets of all departments, she has gone on record that the money spent for cybersecurity is too large in proportion for the size of the company, and she recommends an immediate 23 percent reduction in the cybersecurity budget. She has decided on this amount due to informal conversations she has had with other companies that have about the same number of employees. However, these other companies perform completely different functions: one company is in manufacturing while the other is a service organization, neither of which are the same as your company. She says that she will retract her recommendation if someone can prove that the reason why there have been no significant attacks is due to the money spent on cyber defenses and not just because this company is unattractive to threat actors. Create a one-page memo to the senior vice president that explains your views on cybersecurity spending.

Answer: Answers will vary depending upon the creativity of the learner. The memo should point out that while it is difficult to identify that a preventive measure stopped an attack, nevertheless it is well known that a lack of preventative measures will, given today’s cybersecurity landscape, certainly result in successful attacks.

Security for Life 1: KrebsOnSecurity

Staying abreast of current cybersecurity incidents requires constant vigil. It is important to identify good online resources that you can use to stay current. KrebsOnSecurity (krebsonsecurity.com) has been identified as an excellent resource of current incidents by security researcher and journalist Brian Krebs. Equally valuable are the many comments that other researchers and interested users post.

For this “Security for Life” activity you will read and comment on a posting at KrebsOnSecurity. However, the article that you select must be unique and not an article that another learner has already posted about for this class. For example, suppose you are asked to submit information about the history of your favorite food (that will not be an actual assignment!) and you want to submit information about pizza. Before submitting your information, you will need to read through all previous submissions to be sure that another student has not already submitted information about the history of pizza. If pizza has already been submitted that you must submit a different food.

1. Go to the KrebsOnSecurity site (krebsonsecurity.com) and find an article that is of particular interest to you. It can be any article as long as it has not already been used by another learner.
2. Read the article and also the comments from other users that have been posted on the KrebsOnSecurity site.
3. Go to the discussion feature of the Learning Management System (LMS) used by your school or organization and read the previous postings by other learners.
4. Post a summary (minimum of 200 words) about the article you read. Include information on how the vulnerability was discovered, the risk of the vulnerability, its overall impact, and other pertinent information.
5. Post a reply to another learner’s initial posting (minimum of 50 words).

Grading Rubric for Security for Life

Criteria	Meets Requirements	Needs Improvement	Incomplete
Participation	Submits or participates in discussion by the posted deadlines. Follows all assignment. instructions for initial post and responses. (5 points)	Does not participate or submit discussion by the posted deadlines. Does not follow instructions for initial post and responses. (3 points)	Does not participate in discussion. (0 points)
Contribution Quality	Comments stay on task. Comments add value to discussion topic. Comments motivate other	Comments may not stay on task. Comments may not add value to discussion topic. Comments may not motivate other	Does not participate in discussion. (0 points)

	students to respond. (20 points)	students to respond. (10 points)	
Etiquette	Maintains appropriate language. Offers criticism in a constructive manner. Provides both positive and negative feedback. (5 points)	Does not always maintain appropriate language. Offers criticism in an offensive manner. Provides only negative feedback. (3 points)	Does not participate in discussion. (0 points)

Holistic Score: __________ 4 - **Outstanding** (significantly exceeds expectations); 3 - **Good** (exceeds expectations); 2 - **Fair** (meets basic expectations); 1 - **Poor** (does not meet basic expectations)

Reflection 1: Social Media Profiling

Social engineering impersonation (also called identity fraud) is masquerading as a real or fictitious character and then play out the role of that person on a victim. The more the threat actors know about the person, the more convincing the impersonation will be. Social media profiling is the process of gathering information about a person from one or more social media sites (Facebook, Twitter, Instagram, etc.) that can be used for impersonation. This includes the person's work history, family connections, background, interests, hobbies, skills, and a wide variety of other information a threat actor can use.

1. For this activity, select another learner in your class that you are not already a friend of and ask his or her permission to perform social media profiling. If you are unable to use another learner in your class, select an acquaintance that is in your "outer circle" (not part of your close "inner circle" of friends and family but not a stranger that you have never met).
2. Create a document that outlines the information that you gather on that person along with one or two screen captures of specific information that you have gathered from social media sites.
3. Share that information with the other learner to determine how accurate your information is.
4. Go to the discussion feature of the Learning Management System (LMS) used by your school or organization and post a summary (minimum of 200 words) of your experiences performing a social media profile reconnaissance, including how long it took to perform, how accurate was the information, the reaction of the "victim" when you presented the results, and a tip or trick you learned when performing social media profiling.
5. Respond to one other learner's posting about their experiences (minimum of 50 words).

Grading Rubric for Reflection

Category	Description	Points Possible	Points Earned

Content of Posting	Contains: Summary, length of time to perform, accuracy of information, reaction of victim, and a tip or trick	25	
Format of Posting	Grammar, spelling, punctuation	5	
Content of Response	Polite, concise, informative	15	
Format of Response	Grammar, spelling, punctuation	5	
	Total Points	50	

Holistic Score: __________ 4 - **Outstanding** (significantly exceeds expectations); 3 - **Good** (exceeds expectations); 2 - **Fair** (meets basic expectations); 1 - **Poor** (does not meet basic expectations)