CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

SKU: 9780357678091-TEST-BANK

Name:_____ Class:_____ Date:_____

Module 1 - Enterprise Threats and Vulnerabilities

1. Nik, a cybersecurity analyst, has been asked to examine an employee's iPhone that is exhibiting strange behavior. After looking through the phone, he finds that the user apparently has been able to upload third-party apps that are not in the App Store. Which of the following has most likely occurred with this phone?

a. Rooting
b. Jailbreaking
c. Clapping
d. Raking

ANSWER: b

FEEDBACK:
a. Incorrect. Rooting is a term associated with modifying the operating system or firmware of an Android device, not an iPhone.
b. Correct. Jailbreaking is the term for modifying an iPhone so it can load third-party apps that are not in the App Store.
c. Incorrect. Clapping is a made-up term for the purposes of this scenario.
d. Incorrect. Raking is a made-up term for the purposes of this scenario.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.5 - Explain the threats and vulnerabilities associated with specialized technology.
TOPICS: Threats and Vulnerabilities of Specialized Technology
KEYWORDS: Bloom's: Apply
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 10:33 AM

2. Gabe, a penetration tester, has gained physical access to a company's facilities and planted devices behind several printers that will send him copies of all documents sent to those printers. Which of the following has Gabe executed?

a. MITM attack
b. Replay attack
c. XSS
d. XSRF

ANSWER: a

FEEDBACK:
a. Correct. A man-in-the-middle attack actively intercepts or eavesdrops on communications. By planting a device behind printers, Gabe can capture the data going to the printer and send it outside of the network for later analysis.
b. Incorrect. A replay attack resends captured data to a system in order to perform some other action. In this scenario, Gabe is only capturing the data and sending it outside of the network for analysis.
c. Incorrect. Cross-site scripting does not involve planting devices in an organization.
d. Incorrect. Cross-site request forgery does not involve planting devices in an

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

organization.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
TOPICS: Types of Attacks
KEYWORDS: Bloom's: Apply
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 10:36 AM

3. Lakia has been hired as a penetration tester for a large organization. She finds that one of the branch offices is still running WEP and quickly cracks the key to gain access to the network. As she is capturing network packets while sitting in the company's parking lot, she sees a couple of tokens that users send to an HTTP-based website to log in. Which of the following types of attacks might she be able to perform with this information?

a. XSS
b. Session hijacking
c. XSRF
d. Rootkit attack

ANSWER: b
FEEDBACK:
a. Incorrect. Cross-site scripting does not involve capturing the session token of a user.
b. Correct. Session hijacking is an attack in which a threat actor attempts to impersonate a user by using his session token.
c. Incorrect. Cross-site request forgery does not involve capturing the session token of a user.
d. Incorrect. A rootkit is a type of malware that can hide its presence or the presence of other malware on a computer by accessing lower layers of the operating system or even using undocumented functions to make alterations. It does not involve capturing the session token of a user.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
TOPICS: Types of Attacks
KEYWORDS: Bloom's: Apply
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 10:38 AM

4. Monica wants to implement more security around the login function that her company's website uses to allow

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

customers to interact with the organization. One of the tasks on her to-do list is to prevent brute force attacks. Which of the following might help Monica achieve this goal?

a. Analyze the geolocation where the user is logging in.
b. Analyze the frequency of attempted logins.
c. Analyze the source IP address of the user attempting to log in and ensure that it matches the normal IP address the user logs in from.
d. Analyze the type of device the user is attempting to log in from.

ANSWER: b

FEEDBACK:

a. Incorrect. Nothing in the scenario mentions that users should only be able to log in from certain locations.In a highly mobile world, someone can easily log in from one location and then log in again a few hours later from thousands of miles away.
b. Correct. By analyzing the frequency of attempted logins, Monica might be able to detect whether a brute force attack is being performed by a password cracking program.
c. Incorrect. Users should be able to log in from any device anywhere in the world, as there is not a given requirement to limit the user to connecting from certain networks.
d. Incorrect. Nothing in the scenario states that users are only able to connect from certain types of devices.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
TOPICS: Types of Attacks
KEYWORDS: Bloom's: Apply
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 10:40 AM

5. Frank is analyzing the logs on a server and sees a number of failed attempts using different user accounts. Upon further analysis, he sees that the same password is used for each of the accounts where access was attempted. Which of the following types of attacks has he just discovered on this server?

a. Credential stuffing
b. Session hijacking
c. Man-in-the-middle
d. Password spraying

ANSWER: d

FEEDBACK:

a. Incorrect. Credential stuffing is when an attacker has discovered a list of stolen passwords that have been posted online by threat actors and then uses those passwords across a variety of platforms. Since people commonly re-use the same password on multiple platforms, this gives attackers a high

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

probability of success in gaining access to a user's account.

b. Incorrect. Session hijacking occurs when a threat actor takes over an existing user session. This does not require logging in.

c. Incorrect. Man-in-the-middle attacks do not require logging in, but rather intercept communications between a user and a system.

d. Correct. Password spraying attacks take one or a small number of commonly used passwords and then use that same password when trying to log in to several user accounts.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
TOPICS: Types of Attacks
KEYWORDS: Bloom's: Remember/Understand
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/23/2021 4:08 PM

6. Myleene is analyzing the log files of a publicly available web application that she is responsible for. She sees a number of failed login attempts that have an apostrophe as part of the email address. Which of the following types of attack attempts has she most likely discovered?

a. Buffer overflow attack
b. XML injection
c. SQL injection
d. Integer overflow attack

ANSWER: c
FEEDBACK:

a. Incorrect. In a buffer overflow attack, a process attempts to store data in memory addresses that are beyond the boundaries of a fixed-length storage buffer.

b. Incorrect. Many applications use XML or JSON to structure the data being passed back and forth between various microservices or APIs. By manipulating the XML it is possible to modify the data in the backend database if no input validation or sanitization is performed.

c. Correct. In an SQL injection attack, attackers commonly will use the login portal for web applications with apostrophes included in the username (or email) boxes and / or in the password fields. . If the input is not being sanitized, this could modify the SQL statement that is being passed to the relational database.

d. Incorrect. In an integer overflow attack, the attacker attempts to write a number that is larger than the number allowed for a given field of input in an application

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

Module 1 - Enterprise Threats and Vulnerabilities

LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
TOPICS: Types of Attacks
KEYWORDS: Bloom's: Remember/Understand
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 10:48 AM

7. Masa has just received a call from a number that appears to be one that matches the phone number range of the company that he works for. The person on the other end of the phone states that they are from the IT helpdesk and are performing general system maintenance on all of the user accounts and need to verify his username and password. Which of the following types of attacks has he just been the target of?

a. Piggybacking
b. Whaling
c. Pharming
d. Impersonation

ANSWER: d
FEEDBACK:
a. Incorrect. A piggybacking method of attack involves someone without access to a restricted area following or tagging along with a person who does have access to the restricted area.
b. Incorrect. Whaling is a type of social engineering attack whereby the attacker targets an individual with access to extremely valuable information, who holds a high position of power, or who has considerable monetary resources which the attacker can attempt to get the person to give to the attacker.
c. Incorrect. In a pharming attack, the attacker creates a website that imitates a legitimate website and directs or redirects intended victims to this website in order to gain confidential information from them.
d. Correct. Impersonation is a form of social engineering whereby the attacker pretends to be someone legitimately needing information from the intended victim. The attacker may use various forms of spoofing (including telephone number spoofing) in order to trick the intended victim into thinking that they are legit.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
TOPICS: Types of Attacks
KEYWORDS: Bloom's: Remember/Understand
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/23/2021 4:08 PM

8. Brian is reviewing the logs of a server and notices entries from an internal user attempting to gain accesses to resources to which they do not currently have access. He suspects that the user's account has been

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

compromised. Which of the following types of attacks might he have discovered?

a. Privilege escalation
b. Directory traversal
c. Remote code execution
d. Credential stuffing

ANSWER: a

FEEDBACK:

a. Correct. Privilege escalation is where an attacker attempts to escalate the privileges that they have within a system or gain access to more and more resources. Many times, resources internal to an organization are not as well protected as resources that are public facing, thus increasing the chances of the threat actor's success.
b. Incorrect. Directory traversal is where an attacker can use vulnerabilities, such as the lack of URL query sanitization, in order to execute commands in other directories of a server or system or gain access to the contents of them.
c. Incorrect. Remote code execution is where an attacker has been able to exploit a vulnerability or install tools on a user's system or server that allows the attacker to remotely execute commands on that system, such as through a netcat listener.
d. Incorrect. Credential stuffing is when an attacker has discovered a list of stolen passwords that have been posted online by threat actors and then use those passwords across a variety of platforms. Since people commonly re-use the same password on multiple platforms, this gives attackers a high probability of success in gaining access to a user's account

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.1 - Identify different types of common attacks
ACCREDITING STANDARDS: CIAM.CYSA.22.1.7 - Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
TOPICS: Types of Attacks
KEYWORDS: Bloom's: Remember/Understand
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/23/2021 4:09 PM

9. Lee is a manager for a regional water and sewage utility. The company has a number of devices that help control the flow of water to ensure adequate pressure in various parts of the system as well as ensure that any chemical treatments added are in the appropriate quantities. Which of the following are the types of systems most likely in place so that humans do not have to manually open or close the valves on these systems?

a. ICS
b. IPS
c. IDS
d. IMS

ANSWER: a

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

FEEDBACK:

a. Correct. Industrial control systems manage devices locally or at remote locations by collecting, monitoring, and processing real-time data so that machines can directly control devices such as valves, pumps, and motors without the need for human intervention.

b. Incorrect. An intrusion prevention system can detect intrusions, notify administrators, and enact certain measures in order to stop an attack in progress. They are irrelevant to controlling valves, motors, and other industrial systems.

c. Incorrect. An intrusion detection system can detect intrusions into a network or host and notify an administrator so that the administrator can take the appropriate actions to stop the intrusion.

d. Incorrect. IMS is a made-up term for the purposes of this question.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.3 - Explain security issues of embedded and specialized devices
ACCREDITING STANDARDS: CIAM.CYSA.22.1.5 - Explain the threats and vulnerabilities associated with specialized technology.
TOPICS: Threats and Vulnerabilities of Specialized Technology
KEYWORDS: Bloom's: Apply
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 10:56 AM

10. Which of the following is a vulnerability of using the standard modbus protocol in ICS systems?

a. Since the modbus protocol has been incorporated to use TCP/IP it is no longer able to poll multiple devices at one time; it now must poll each device individually.

b. The standard modbus protocol includes a weak form of encryption that has never been upgraded to the more advanced forms of encryption available today.

c. While the modbus protocol includes checksums, it does not include protections against injected commands or the interception of data.

d. The standard modbus protocol requires older versions of the Windows operating system, leading companies using these systems to delay upgrades due to the increased cost of upgrading more components than just the ICS system itself.

ANSWER: c

FEEDBACK:

a. Incorrect. The original modbus protocol polled each device sequentially.

b. Incorrect. The standard modbus protocol does not include any forms of encryption—weak or otherwise.

c. Correct. The standard modbus protocol includes checksums to ensure that the data received is the data that was sent. However, it does not include protections against injected commands or the interception of data.

d. Incorrect. The standard modbus protocol does not require the Windows operating system.

POINTS: 1
QUESTION TYPE: Multiple Choice

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

Module 1 - Enterprise Threats and Vulnerabilities

HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.3 - Explain security issues of embedded and specialized devices
ACCREDITING STANDARDS: CIAM.CYSA.22.1.5 - Explain the threats and vulnerabilities associated with specialized technology.
TOPICS: Threats and Vulnerabilities of Specialized Technology
KEYWORDS: Bloom's: Apply
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 10:59 AM

11. Tamela has a number of ICS systems throughout the manufacturing plant where she works. She is looking for a way to control all of them so she doesn't have to manage so many individual systems. Which of the following might she choose to implement in order to meet this objective?

a. MICS
b. SCADA
c. CAPS
d. IMAP

ANSWER: b
FEEDBACK:
a. Incorrect. MICS is a made-up term for the purposes of this question.
b. Correct. Supervisory Control and Data Acquisition (SCADA) systems can manage multiple industrial control systems (ICS). They can help maintain efficiency and provide information on issues to help reduce downtime.
c. Incorrect. CAPS is a made-up term for the purposes of this question.
d. Incorrect. IMAP is the Internet Mail Access Protocol and is irrelevant to managing industrial control systems.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.3 - Explain security issues of embedded and specialized devices
ACCREDITING STANDARDS: CIAM.CYSA.22.1.5 - Explain the threats and vulnerabilities associated with specialized technology.
TOPICS: Threats and Vulnerabilities of Specialized Technology
KEYWORDS: Bloom's: Remember/Understand
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 11:01 AM

12. Lauranne has just installed a new network-connected thermostat at her home so that she more easily can control the temperatures in the house while working from home during a pandemic without having to leave the room where her home office is located. Which of the following is the best term that can be applied to these types of devices?

a. IoT
b. SCADA

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

c. CAN bus
d. FPGA

ANSWER: a

FEEDBACK:
a. Correct. The Internet of Things has been defined by the ITU-T as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.
b. Incorrect. Supervisory Control and Data Acquisition systems manage industrial control systems (ICS).
c. Incorrect. The CAN (controller area network) bus network is used by the automobile sector for sending and receiving data throughout the automobile to a variety of sensors and components.
d. Incorrect. A field-programmable gate array is a hardware chip or integrated circuit that can be programmed by the user to carry out one or more logical operations.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.CYSA.22.1.3 - Explain security issues of embedded and specialized devices
ACCREDITING STANDARDS: CIAM.CYSA.22.1.5 - Explain the threats and vulnerabilities associated with specialized technology.
TOPICS: Threats and Vulnerabilities of Specialized Technology
KEYWORDS: Bloom's: Remember/Understand
DATE CREATED: 7/9/2021 3:31 PM
DATE MODIFIED: 7/19/2021 11:05 AM

13. Ryenne works for an automobile manufacturer that constantly tests new technologies on a racetrack that is shielded from view of neighboring properties and roads. However, she is concerned with the proliferation of new devices that easily could allow unauthorized persons to spy on the products that they are testing. Which of the following describes the types of devices about which Ryenne is concerned?

a. OFO
b. UFO
c. AFV
d. UAV

ANSWER: d

FEEDBACK:
a. Incorrect. OFO is a made-up acronym for the purposes of this question.
b. Incorrect. While these may technically be unidentified flying objects initially because the company cannot determine who owns them, they are typically readily identified as drones, or unmanned aerial vehicles.
c. Incorrect. AFV is a made-up acronym for the purposes of this question.
d. Correct. Unmanned aerial vehicles

POINTS: 1
QUESTION TYPE: Multiple Choice

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank

Module 1 - Enterprise Threats and Vulnerabilities

HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.CYSA.22.1.3 - Explain security issues of embedded and specialized devices
ACCREDITING STANDARDS:	CIAM.CYSA.22.1.5 - Explain the threats and vulnerabilities associated with specialized technology.
TOPICS:	Threats and Vulnerabilities of Specialized Technology
KEYWORDS:	Bloom's: Remember/Understand
DATE CREATED:	7/9/2021 3:31 PM
DATE MODIFIED:	7/19/2021 11:07 AM

14. Krishna works for a vehicle manufacturer that is continuing to automate and re-engineer certain functions on its vehicles to require less human control and interaction. Which of the following is the term for the networks on these vehicles that connect the components together?

a. ECN
b. UAV
c. CAN
d. ECU

ANSWER: c

FEEDBACK:

a. Incorrect. ECN is a made-up term for the purposes of this question.
b. Incorrect. Unmanned aerial vehicles are also known as drones.
c. Correct. The controller area network (CAN) bus network sends and receives data from various components and ECUs (electronic control units) within a vehicle.
d. Incorrect. Electronic control units receive data from sensors and control other devices throughout the vehicle using the input from the sensors.

POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.CYSA.22.1.3 - Explain security issues of embedded and specialized devices
ACCREDITING STANDARDS:	CIAM.CYSA.22.1.5 - Explain the threats and vulnerabilities associated with specialized technology.
TOPICS:	Threats and Vulnerabilities of Specialized Technology
KEYWORDS:	Bloom's: Remember/Understand
DATE CREATED:	7/9/2021 3:31 PM
DATE MODIFIED:	7/19/2021 11:09 AM

Copyright Cengage Learning. Powered by Cognero.

CompTIA CySA Guide to Cybersecurity Analyst CS0 002 2nd edition Ciampa Test Bank