Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Name:_____ Class:_____ Date:_____

Mod 01: Introduction to Security

1. Which type of threat actor would benefit the most from accessing your enterprise's new machine learning algorithm research and development program?

a. Shadow IT
b. Brokers
c. Criminal syndicates
d. Competitors

ANSWER: d

FEEDBACK:

a. Incorrect. Shadow IT are employees of the enterprise frustrated with the pace of acquiring new technology.
b. Incorrect. Brokers sell their knowledge of a security weakness to other attackers or governments.
c. Incorrect. Criminal syndicates are threat actors who involve experienced online criminals who do not commit crimes themselves but acts as entrepreneurs.
d. Correct. Competitors are threat actors who launch attacks against an opponent's system to steal classified information like industry research or customer lists.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.2 - Identify threat actors and their attributes
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Who Are the Threat Actors?
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

2. Which of the following types of platforms is known for its vulnerabilities due to age?

a. On-premises platform
b. Cloud platform
c. Legacy platform
d. Online platform

ANSWER: c

FEEDBACK:

a. Incorrect. On-premises platforms ("on-prem") are the software and technology located within an enterprise's physical confines, usually consolidated in the company's data center.
b. Incorrect. Cloud platforms are a new model gaining widespread use. They are a pay-per-use computing model in which customers pay only for the online computing resources they need.
c. Correct. Legacy platforms are no longer in widespread use, often because they have been replaced by an updated version of the earlier technology.
d. Incorrect. An online platform is one that has its front end and back end online.

POINTS: 1

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Name:_____ Class:_____ Date:_____

Mod 01: Introduction to Security

QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS:	SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS:	Vulnerabilities and Attack
KEYWORDS:	Bloom's: Remember
DATE CREATED:	2/16/2022 10:23 PM
DATE MODIFIED:	2/16/2022 10:23 PM

3. Your enterprise has played fast and loose with customer information for years. While there has been no significant breach of information that could damage the organization and/or their customers, many in the enterprise feel it is only a matter of time before a major leak occurs.

Which type of threat actor is an employee who wishes to personally ensure that the enterprise is exposed and blocked from accessing their customers' information until they ensure more secure protocols?

a. Hacktivist
b. Insider
c. State actor
d. Script kiddy

ANSWER: a

FEEDBACK:

a. Correct. A hacktivist is strongly motivated by ideology for the sake of their principles or beliefs.
b. Incorrect. This serious threat to an enterprise comes from its own employees, contractors, and business partners, called insiders. They pose an insider threat of manipulating data from the position of a trusted employee.
c. Incorrect. These types of actors are employed by governments for launching cyberattacks against their foes.
d. Incorrect. Script kiddies do their work by downloading freely available automated attack software (scripts) and using it to perform malicious acts.

POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.1.2 - Identify threat actors and their attributes
ACCREDITING STANDARDS:	SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS:	Who Are the Threat Actors?
KEYWORDS:	Bloom's: Apply
DATE CREATED:	2/16/2022 10:23 PM
DATE MODIFIED:	2/16/2022 10:23 PM

4. Threat actors focused on financial gain often attack which of the following main target categories?

a. Product lists
b. Individual users

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

c. Social media assets
d. REST services

ANSWER: b

FEEDBACK:

a. Incorrect. Product lists could be used for many things, but they are not a main target of attacks motivated by financial gain.
b. Correct. This category focuses on individuals as the victims. Threat actors steal and use data, credit card numbers, online financial account information, or social security numbers or send millions of spam emails to peddle counterfeit drugs, pirated software, fake watches, and pornography to profit from their victims.
c. Incorrect. Social media assets are attacked but do not fall into one of the main categories.
d. Incorrect. REST services could be a potential sub-level target but are not considered one of the main categories.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.2 - Identify threat actors and their attributes
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Who Are the Threat Actors?
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

5. Which issue can arise from security updates and patches?

a. Difficulty patching firmware
b. Difficulty updating settings
c. Difficulty resetting passwords
d. Difficulty installing databases

ANSWER: a

FEEDBACK:

a. Correct. Updating firmware to address a vulnerability can often be difficult and requires specialized steps. Furthermore, some firmware cannot be patched.
b. Incorrect. While a potential difficulty in some situations, updating most settings is an easy change in many cases.
c. Incorrect. Resetting passwords is not included in updates and patches.
d. Incorrect. Installing databases is not a function of security updates.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS: Vulnerabilities and Attacks

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Mod 01: Introduction to Security

KEYWORDS: Bloom's: Remember
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

6. Which of the following is an attack vector used by threat actors to penetrate a system?

a. Phishing
b. Intimidation
c. Urgency
d. Email

ANSWER: d

FEEDBACK:

a. Incorrect. Phishing is a specific type of attack but not an actual vector type.
b. Incorrect. Intimidation might be used to scare someone into giving information but is not a type of vector.
c. Incorrect. Urgency is a psychological-based social engineering tactic used to get the victim to give up sensitive information; it is not an attack vector type.
d. Correct. Almost 94 percent of all malware is delivered through email to an unsuspecting user. The goal is to trick the user into opening an attachment that contains malware or click on a hyperlink that takes the user to a fictitious website.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Vulnerabilities and Attacks
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

7. What is a variation of a common social engineering attack targeting a specific user?

a. Spear phishing
b. Redirection
c. Spam
d. Watering holes
e. Correct. Spear phishing targets specific users. The emails used in spear phishing are customized to the recipients, including their names and personal information, to make the message appear legitimate.
f. Incorrect. Threat actors use redirection to get users to click on or visit a fake site. These attacks are not targeted at specific users.
g. Incorrect. Spamming is a lucrative means of sending unsolicited emails to several recipients. The cost of sending millions of spam email messages is meager, and the potential payoff can be high.
h. Incorrect. A watering hole attack is directed towards a smaller group of specific individuals, such as

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

the executives working for a manufacturing company. These executives all tend to visit common websites, such as supplier sites. An attacker who wants to target this group of executives infects the commonly used site with malware that will then make its way onto the group's computers and networks.

ANSWER:	h
POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS:	SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS:	Vulnerabilities and Attacks
KEYWORDS:	Bloom's: Remember
DATE CREATED:	2/16/2022 10:23 PM
DATE MODIFIED:	2/16/2022 10:23 PM

8. Which of the following is a social engineering method that attempts to influence the subject before the event occurs?

a. Spear phishing
b. Redirection
c. Prepending
d. Watering hole
e. Incorrect. Spear phishing targets specific users. The emails used in spear phishing are customized to the recipients, including their names and personal information, to make the message appear legitimate.
f. Incorrect. If threat actors cannot trick a user into visiting a malicious website through phishing, they can use other tactics to redirect users to fake websites.
g. Correct. Prepending attempts to influence the subject before the attack event occurs. A common general example is a preview of a soon-to-be-released movie that begins with the statement, "The best film you will see this year!" Threat actors use prepending with social engineering attacks, such as including the desired outcome in a statement that uses the urgency principle, as in "You need to reset my password immediately because my meeting with the board starts in five minutes."
h. Incorrect. A watering hole attack is directed towards a smaller group of specific individuals, such as the top executives working for a manufacturing company. These executives all tend to visit common websites, such as supplier sites. An attacker who wants to target this group of executives infects the commonly used site with malware that will then make its way onto the group's computers and networks.

ANSWER:	h
POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS:	SY0-601.1.1 - Compare and contrast different types of social engineering attacks.

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Mod 01: Introduction to Security

TOPICS: Vulnerabilities and Attacks
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

9. Which attack embeds malware-distributing links in instant messages?

a. Spam
b. Spim
c. Phishing
d. Tailgating
e. Incorrect. Spam involves sending millions of unsolicited emails to a large number of companies and/or recipients.
f. Correct. Spim is spam delivered through an IM service instead of email.
g. Incorrect. Phishing is the social engineering process of sending email messages or displaying a web announcement that falsely claims to be from a legitimate enterprise to trick a user into giving information or taking action.
h. Incorrect. Once an authorized person opens the door, one or more individuals can follow behind and also enter. This is known as tailgating.

ANSWER: h
POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS: Vulnerabilities and Attacks
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

10. Your enterprise experienced several technical issues over the last few days. There were multiple instances of passwords needing to be changed and other issues causing downtime. Management has started receiving voicemails regarding fraudulent activities on their accounts. While the voicemails sound authentic, the help desk concludes that they are fake.

What type of malicious activity will this be considered?

a. Spimming
b. Whaling
c. Spamming
d. Vishing
e. Incorrect. Spim is spam delivered through instant messaging (IM) instead of email.
f. Incorrect. Whaling is a type of spear phishing that goes after big fishes like wealthy individuals or

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

senior executives.

g. Incorrect. Spam involves sending millions of unsolicited emails to a large volume of companies and/or recipients.

h. Correct. Instead of using email to contact the potential victim, attackers can use phone calls. Known as vishing (voice phishing), an attacker calls a victim who, upon answering, hears a recorded message that pretends to be from the user's bank stating that their credit card shows fraudulent activity or that the bank account shows unusual activity. The victim is instructed to immediately call a specific phone number (which the attacker has set up). When the victim calls, it is answered by automated instructions telling them to enter their credit card number, bank account number, social security number, or other information on the phone's keypad.

ANSWER:	h
POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS:	SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS:	Vulnerabilities and Attacks
KEYWORDS:	Bloom's: Apply
DATE CREATED:	2/16/2022 10:23 PM
DATE MODIFIED:	2/16/2022 10:23 PM

11. Attackers have taken over a site commonly used by an enterprise's leadership team to order new raw materials. The site is also visited by leadership at several other enterprises, so infecting this site will allow for attacks on many organizations.

Which type of malicious activity is this?

a. Spear phishing

b. Hoax

c. Watering hole

d. Vishing

e. Incorrect. Spear phishing targets specific users. The emails used in spear phishing are customized to the recipients, including their names and personal information, to make the message appear legitimate.

f. Incorrect. A hoax is a false warning, often contained in an email message claiming to come from the IT department. The hoax purports a "deadly virus" circulating through the internet and that the recipient should erase specific files or change security configurations and then forward the message to other users.

g. Correct. A watering hole attack is directed towards a smaller group of specific individuals, such as the top executives working for a manufacturing company. These executives all tend to visit a common website, such as a parts supplier to the manufacturer. An attacker who wants to target this group of executives tries to determine the common website they frequent and then infects it with malware that will make its way onto the group's computers.

h. Incorrect. Instead of using email to contact the potential victim, attackers can use phone calls. Known

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

as vishing (voice phishing), an attacker calls a victim who, upon answering, hears a recorded message that pretends to be from the user's bank stating that her credit card has experienced fraudulent activity or that her bank account has had unusual activity. The victim is instructed to immediately call a specific phone number (which the attacker has set up). When the victim calls, it is answered by automated instructions telling her to enter her credit card number, bank account number, social security number, or other information on the phone's keypad.

ANSWER: h
POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS: Vulnerabilities and Attacks
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

12. Over the last few days, several employees in your enterprise reported seeing strange messages containing links in their company's IM account. Even though no one has clicked on the messages, they are spreading throughout the network.

Which type of malicious activity is this?

a. Spear phishing
b. Whaling
c. Spimming
d. Vishing
e. Incorrect. Spear phishing targets specific users. The emails used in spear phishing are customized to the recipients, including their names and personal information, to make the message appear legitimate.
f. Incorrect. Whaling is a type of spear phishing that goes after big fish like wealthy individuals or senior executives.
g. Correct. Spim is spam delivered through instant messaging (IM) instead of email. For threat actors, spim can have even more impact than spam. The immediacy of instant messages makes users more likely to reflexively click embedded links in a spim.
h. Incorrect. Instead of using email to contact the potential victim, attackers can use phone calls. Known as vishing (voice phishing), an attacker calls a victim who, upon answering, hears a recorded message that pretends to be from the user's bank stating that her credit card has experienced fraudulent activity or that her bank account has had unusual activity. The victim is instructed to immediately call a specific phone number (which the attacker has set up). When the victim calls, it is answered by automated instructions telling her to enter her credit card number, bank account number, social security number, or other information on the phone's keypad.

ANSWER: h
POINTS: 1

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Mod 01: Introduction to Security

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS: Vulnerabilities and Attacks
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

13. Which threat actors sell their knowledge to other attackers or governments?

a. Brokers
b. Cyberterrorists
c. Competitors
d. Criminal syndicates

ANSWER: a
FEEDBACK:
a. Correct. Brokers sell their knowledge of a weakness to other attackers or governments.
b. Incorrect. Cyberterrorists attack a nation's network and computer infrastructure to cause disruption and panic among citizens.
c. Incorrect. Competitors launch attacks against an opponent's system to steal classified information.
d. Incorrect. Criminal syndicates move from traditional criminal activities to more rewarding and less risky online attacks.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Who Are the Threat Actors?
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

14. Which of the following is the most common method for delivering malware?

a. Removable media
b. Social media
c. Email
d. Identity theft
e. Incorrect. A removable media device, such as a USB flash drive, is a common attack vector. Threat actors have been known to infect USB flash drives with malware and leave them scattered in a parking lot or cafeteria; however, this is not the most common method for delivering malware.
f. Incorrect. Social media is not the most common method for delivering malware. Threat actors often

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

use social media as a vector for attacks. For example, an attacker may read social media posts to determine when an employee will be on vacation and then call the organization's help desk pretending to be that employee to ask for "emergency" access to an account.

g. Correct. Almost 94 percent of all malware is delivered through email to an unsuspecting user. The goal is to trick the user into opening an attachment that contains malware or click a hyperlink that takes the user to a fictitious website.

h. Incorrect. Identify theft is often the goal of social engineering attacks. It involves taking someone's personally identifiable information to impersonate them.

ANSWER: h
POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

15. Which of the following computing platforms is highly vulnerable to attacks?

a. On-premises
b. Cloud
c. Legacy
d. Hybrid

ANSWER: c
FEEDBACK:

a. Incorrect. On-premises platforms are not highly vulnerable compared to other platforms, as on-prem networks are kept up-to-date by security personnel.
b. Incorrect. Cloud platforms are not as vulnerable as other platforms, as they use new technologies.
c. Correct. Old and outdated computing resources used in legacy platforms make them highly vulnerable.
d. Incorrect. Hybrid platforms are a combination of on-prem and cloud platforms. They are not highly vulnerable when compared to other platforms.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

16. Your company is considering updating several electronic devices used in the enterprise network. The third-party service provider that your company approached says that they require access to the enterprise network in order to implement the updates. As the chief information security officer, you are asked to analyze the requirement and submit a report on potential vulnerabilities when giving a third-party access to the network.

Which of the following vulnerabilities should you list as the most likely to affect the enterprise network?

a. Zero day
b. Weakest link
c. Weak encryption
d. Default settings

ANSWER: b

FEEDBACK:

a. Incorrect. A zero-day vulnerability is a vulnerability present in a software that is found by an outsider, not the developer.
b. Correct. The enterprise network is highly vulnerable to the weakest link on the integration of a third-party. That is, if the third-party's security has any weaknesses, it can provide an opening for attackers to infiltrate the enterprise network.
c. Incorrect. Using weak encryption is a configuration vulnerability. This vulnerability is less likely to occur in relation to third-party integration with a network.
d. Incorrect. Using default settings is a configuration vulnerability. This vulnerability is less likely to occur in relation to third-party integration with a network.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

17. What is an officially released software security update intended to repair a vulnerability called?

a. Firmware
b. Vector
c. Patch
d. Default

ANSWER: c

FEEDBACK:

a. Incorrect. Firmware is software that is embedded into hardware.
b. Incorrect. Vectors are not software security updates.

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

c. Correct. A security patch is an officially released software security update intended to repair a vulnerability.

d. Incorrect. Defaults or default settings are the settings predetermined by a vendor for usability and ease of use.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

18. Your company recently purchased routers with new and updated features and deployed them in the highly secure enterprise network without changing the default settings. A few days later, the enterprise network suffered a data breach, and you are assigned to prepare a report on the data breach. Which of the following vulnerabilities should you identify as the source of the breach?

a. Platform vulnerability
b. Configuration vulnerability
c. Third-party vulnerability
d. Zero-day vulnerability

ANSWER: b
FEEDBACK:

a. Incorrect. Platform vulnerabilities are the result of platforms being used as high security. Maintained in the enterprise network, platform vulnerabilities are less likely to occur.

b. Correct. As the routers were deployed without changing configuration from the default settings, threat actors might have gained easy access to the enterprise network.

c. Incorrect. There is nothing in this scenario that indicates the enterprise uses third-party vendors; it is unlikely the breach was caused by a third-party vulnerability.

d. Incorrect. Zero-day vulnerabilities are associated with unknown vulnerabilities present in a software.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/16/2022 10:23 PM

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Mod 01: Introduction to Security

DATE MODIFIED: 2/16/2022 10:23 PM

19. Zero-day vulnerabilities and configuration vulnerabilities can heavily impact a system if exploited. How should you differentiate between a zero-day vulnerability and a configuration vulnerability?

a. A zero-day vulnerability results from improper hardware configurations, whereas a configuration vulnerability results from improper software configuration.
b. A zero-day vulnerability is an easily fixable vulnerability recognized by a software developer, whereas a configuration vulnerability is a major vulnerability present in a system exploited by a threat actor before the software developer can fix it.
c. A zero-day vulnerability is an unknown vulnerability in released software that is found and exploited by a threat actor, whereas a configuration vulnerability is caused by improper settings in hardware or software.
d. A zero-day vulnerability results from users improperly configuring software, whereas a configuration vulnerability results from the developers improperly configuring the software.

ANSWER: c

FEEDBACK:

a. Incorrect. A zero-day vulnerability is not a result of improper hardware configuration. A configuration vulnerability can be caused by improper software configurations.
b. Incorrect. A zero-day vulnerability is not uncovered by the developer and exploited by the threat actor, and it might not be easily fixable. A configuration vulnerability is not a built-in vulnerability exposed and exploited by threat actors before developers can fix it.
c. Correct. A zero-day vulnerability is uncovered first by threat actors, who exploit it to penetrate systems. A configuration vulnerability occurs when a user misconfigures the system or fails to configure it past the default settings.
d. Incorrect. A zero-day vulnerability is not caused by users misconfiguring the system. A configuration vulnerability is not caused by the developers or designers.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

20. In an interview, the interviewer introduced the following scenario:
An enterprise is hosting all its computing resources on a cloud platform, and you need to identify which vulnerability is most likely to occur.

Which of the following should you choose?

a. Physical access vulnerability

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Mod 01: Introduction to Security

b. Configuration vulnerability
c. Zero-day vulnerability
d. Third-party vulnerability

ANSWER: b

FEEDBACK:

a. Incorrect. Since the resources are hosted in the cloud, they are likely well-protected from threat actors gaining physical access to them.
b. Correct. Misconfiguration vulnerabilities are often found in cloud platforms, as company personnel responsible for securing the platform might improperly configure the resources, resulting in a vulnerability.
c. Incorrect. Zero-day vulnerabilities are not specific to cloud platforms. They are software-based vulnerabilities that are discovered first by threat actors before anyone else even knows they exist.
d. Incorrect. Third-party access vulnerabilities are not the most likely in this scenario.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

21. Which of the following is a configuration vulnerability?

a. Weakest link
b. Weak encryption
c. Zero day
d. Direct access

ANSWER: b

FEEDBACK:

a. Incorrect. Weakest-link vulnerabilities are caused by allowing an unsecured third party to access systems.
b. Correct. Weak encryption is a configuration vulnerability caused by a user selecting an encryption scheme with a known weakness or a key value that is too short or by a user not changing the default configuration settings.
c. Incorrect. Zero-day vulnerabilities are not configuration vulnerabilities, as they result from improper design or development of software.
d. Incorrect. Patches are fixes that address certain vulnerabilities.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.6 - Explain the security concerns associated with various types of

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

	vulnerabilities.
TOPICS:	Vulnerabilities and Attack
KEYWORDS:	Bloom's: Understand
DATE CREATED:	2/16/2022 10:23 PM
DATE MODIFIED:	2/16/2022 10:23 PM

22. You work for an enterprise that provides various cybersecurity services. You are assigned to examine an enterprise's network and suggest security measures modifications, if necessary. On examining the network, you find that the enterprise hosts most of its computing resources on a cloud platform and few resources on-premises, and both seem to have secure settings implemented. You also find that the enterprise computers use the Windows XP operating system.

Which of the following vulnerabilities should you insist on fixing first?

a. Platform vulnerability
b. Configuration vulnerability
c. Zero-day vulnerability
d. Third-party vulnerability

ANSWER: a

FEEDBACK:

a. Correct. Platform vulnerability is present in the network, as the enterprise's computers use a legacy operating system.
b. Incorrect. Because the cloud and on-premises platforms are secured through settings, it is unlikely that there are many, if any, configuration vulnerabilities in the system.
c. Incorrect. Zero-day vulnerabilities are not identified by examining enterprise networks, as they are specific to various software and are found and exploited by threat actors before anyone else knows they exist.
d. Incorrect. There is no indication that a third party was authorized to access the network, so the enterprise network is not vulnerable to third-party access.

POINTS:	1
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS:	SY0-601.1.6 - Explain the security concerns associated with various types of vulnerabilities.
TOPICS:	Vulnerabilities and Attack
KEYWORDS:	Bloom's: Apply
DATE CREATED:	2/16/2022 10:23 PM
DATE MODIFIED:	2/16/2022 10:23 PM

23. An unauthorized person recently accessed your enterprise network. The security team had received a call from the threat actor claiming to be a higher official. They followed the attacker's instructions to log them onto a specific webpage, leading to the exposure of enterprise network credentials.

Which of the following social engineering techniques was used here?

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

a. Hoaxes and impersonation
b. Spam and phishing
c. Impersonation and phishing
d. Hoaxes and spam

ANSWER: c

FEEDBACK:

a. Incorrect. A hoax is a false warning, often contained in an email message claiming to come from the IT department; no such message was used in this scenario.
b. Incorrect. Spam and phishing both use unsolicited emails sent to a large volume of recipients with different attack goals.
c. Correct. Here, the threat actor impersonated a higher official at an organization to trick the security team into logging on to a phishing webpage through which the attacker was able to access enterprise network credentials.
d. Incorrect. A hoax is a false warning, often contained in an email message claiming to come from the IT department. Spam involves sending a large volume of unsolicited emails to a large volume of recipients. These techniques were not used in this scenario.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.4 - Explain the impact of attacks
ACCREDITING STANDARDS: SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

24. Social engineering is a means of eliciting information by relying on the weaknesses of individuals. How should you differentiate between the social engineering techniques of phishing and pharming?

a. Phishing involves sending millions of generic email messages to a large volume of users, whereas pharming targets specific users by sending emails customized to the recipients, including their names and personal information.
b. Phishing involves sending customized emails to recipients, including their names and personal information, to make the message appear legitimate, whereas pharming is a variant of phishing that specifically targets wealthy individuals or senior executives within a business.
c. Phishing involves sending an email message or displaying a web announcement that falsely claims to be from a legitimate enterprise, whereas pharming is a redirection technique that attempts to exploit how a URL is converted into its corresponding IP.
d. Phishing involves digging through trash receptacles to find information that can be useful in an attack, whereas pharming involves sending millions of unsolicited emails to a large volume of users.

ANSWER: c

FEEDBACK:

a. Incorrect. Spear phishing targets specific users by sending emails customized to the recipients, including their names and personal information.
b. Incorrect. Spear phishing targets specific users. Whaling is a variant of spear

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

phishing that targets wealthy individuals.

c. Correct. Phishing involves sending an email message or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information or taking action. Pharming is a redirection technique that attempts to exploit a URL by converting its corresponding IP address. A threat actor may install malware on a user's computer that redirects traffic away from its intended target to a fake website instead.

d. Incorrect. Dumpster diving is a physical social engineering technique that involves digging through trash receptacles to find information. Spamming is a psychological social engineering technique that sends millions of unsolicited emails to a large volume of users.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

25. Which of the following is a physical social engineering technique?

a. Pharming
b. Watering hole
c. Dumpster diving
d. Hoaxes

ANSWER: c
FEEDBACK:

a. Incorrect. Pharming is a psychological redirection technique through which the user is unknowingly redirected to a malicious website.

b. Incorrect. Watering hole attacks use psychological principles to direct attacks toward a small group of specific individuals.

c. Correct. Dumpster diving involves digging through trash receptacles to find information that can be useful in an attack.

d. Incorrect. A hoax is a psychological approach in which a false warning to update settings is made, often in an email message, purportedly by the IT department.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/16/2022 10:23 PM

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

Mod 01: Introduction to Security

DATE MODIFIED: 2/16/2022 10:23 PM

26. Several websites use URLs similar to one of the most globally popular websites, attempting to attract traffic if a user misspells the popular website's URL. What is this social engineering technique called?

a. Pharming
b. Spam
c. Tailgating
d. Typo squatting

ANSWER: d

FEEDBACK:

a. Incorrect. Pharming is a redirection technique that attempts to exploit how a URL is converted into its corresponding IP.
b. Incorrect. Spam is unsolicited emails sent to a large number of recipients.
c. Incorrect. Tailgating involves following legitimate users through security checkpoints to gain unauthorized physical access to systems.
d. Correct. Typo squatting involves creating websites with URLs similar to websites with high traffic in an attempt to redirect users who mistype the intended URL.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.1 - Compare and contrast different types of social engineering attacks.
TOPICS: Vulnerabilities and Attack
KEYWORDS: Bloom's: Understand
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

27. Which threat actors violate computer security for personal gain?

a. White hat hackers
b. Gray hat hackers
c. Black hat hackers
d. Red hat hackers

ANSWER: c

FEEDBACK:

a. Incorrect. White hat hackers attempt to probe a system (with an organization's permission) for weaknesses and then privately provide their results to the organization.
b. Incorrect. Gray hat hackers are attackers who attempt to break into a computer system without the organization's permission (an illegal activity), not for their own advantage, but to shame an organization into taking action.
c. Correct. Black hat hackers are threat actors who violate computer security for personal gains, such as to steal credit card numbers or to inflict malicious damage.
d. Incorrect. Red hat hackers are similar to white hats. They are vigilantes who target black hat hackers, forcing them to stop their attacks or revealing their

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

identities. Red hat hackers rarely report malicious hackers to authorities, preferring to use aggressive means like DoS attacks or planting viruses against black hat hackers.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Who Are the Threat Actors?
KEYWORDS: Bloom's: Remember
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

28. A federal appeals court recently made a judgment that caused significant public outrage. Soon after the ruling, the court's website was hacked, and the content was replaced with the text "Equal justice for all."

Which of the following type of threat actors attacked the court's site?

a. Insiders
b. Cyberterrorists
c. Hacktivists
d. State actors

ANSWER: c
FEEDBACK:

a. Incorrect. Insiders do not attack government resources for political reasons.
b. Incorrect. Cyberterrorists attack a nation's network and computer infrastructure to cause disruption and panic among citizens.
c. Correct. Hacktivists are individuals who attack a computer system or network for socially or politically motivated reasons.
d. Incorrect. State actors are sponsored by a government to perform an attack on its enemies.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Who Are the Threat Actors?
KEYWORDS: Bloom's: Apply
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

29. In cybersecurity, a threat actor is an individual or an entity responsible for cyber incidents against the technical equipment of enterprises and users. How should you differentiate an attack by a script kiddie from that of a gray hat hacker?

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

a. Script kiddies construct efficient scripts to perform attacks to fulfill their own needs, whereas gray hat hackers construct scripts for attacking organizational competitors.
b. Script kiddies lack the technical knowledge to carry out attacks, so they hire a hacker to do it, whereas gray hat hackers violate computer security to fulfill their financial needs.
c. Script kiddies are hired to probe systems for weaknesses and then privately provide that information back to the organization, whereas gray hat hackers break into systems for ideological or political reasons.
d. Script kiddies use automated attack software created by other hackers for personal gain, whereas gray hat hackers create their own attack software to showcase vulnerabilities present in a system to the world.

ANSWER: d

FEEDBACK:

a. Incorrect. Script kiddies do not have the technical knowledge required to construct their own scripts, and gray hat hackers don't attack organizational competitors.
b. Incorrect. Script kiddies do not hire other hackers to perform their attacks, and gray hat hackers do not use technical knowledge for personal gain.
c. Incorrect. Ethical hackers, or white hat hackers, attempt to probe a system for weaknesses and then privately provide that information back to the organization, and hacktivist attacks are motivated by ideologies.
d. Correct. Script kiddies lack the technical knowledge to carry out hacking attacks. Instead, script kiddies use freely available scripts that they can download off the internet. Gray hat hackers attempt to break into a computer system without the organization's permission but not for their own advantage. Instead, they publicly disclose the attack in order to shame the organization into taking action.

POINTS: 1
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks
ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.
TOPICS: Who Are the Threat Actors?
KEYWORDS: Bloom's: Analyze
DATE CREATED: 2/16/2022 10:23 PM
DATE MODIFIED: 2/16/2022 10:23 PM

30. Hacktivists and state actors are huge threats to government systems. What is the main difference between hacktivists and state actors?

a. Hacktivists are covertly sponsored by a government to attack its foes, whereas state actors misuse a computer system or network for personal, social, or political reasons.
b. Hacktivists misuse a computer system or network for socially or politically motivated reasons, whereas state actors are covertly sponsored by a government to attack its foes.
c. Hacktivists attack their own enterprise network for political revenge or personal gain, whereas state actors attack a nation's network and computer infrastructure to cause disruption and panic among citizens.
d. Hacktivists attack a nation's network and computer infrastructure to cause disruption and panic

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa

among citizens, whereas state actors attack their own enterprise network for political revenge or personal gain.

ANSWER: b

FEEDBACK:

a. Incorrect. Hacktivists are not sponsored by governments to perform attacks on their enemies, and state actors don't attack for personal, social, or political reasons.

b. Correct. Hacktivists misuse a computer system or network for socially or politically motivated reasons. Instead of using an army to march across the battlefield to strike an adversary, governments increasingly employ their own state-sponsored attackers to launch cyberattacks against their foes. These attackers are known as state actors.

c. Incorrect. Insiders attack their own enterprise networks, and cyberterrorists attack a nation's network and computer infrastructure to cause disruption and panic among citizens.

d. Incorrect. Cyberterrorists attack a nation's network and computer infrastructure to cause disruption and panic among citizens, and insiders attack their own enterprise network.

POINTS: 1

QUESTION TYPE: Multiple Choice

HAS VARIABLES: False

LEARNING OBJECTIVES: CIAM.SEC+.22.1.3 - Describe the different types of vulnerabilities and attacks

ACCREDITING STANDARDS: SY0-601.1.5 - Explain different threat actors, vectors, and intelligence sources.

TOPICS: Who Are the Threat Actors?

KEYWORDS: Bloom's: Analyze

DATE CREATED: 2/16/2022 10:23 PM

DATE MODIFIED: 2/16/2022 10:23 PM

Copyright Cengage Learning. Powered by Cognero.

Access Complete Test Bank for CompTIA Security Guide to Network Security Fundamentals 7th Ciampa