Vendor: (ISC)2

Exam Code: Certified-in-Cybersecurity

Exam Name: ISC2 CC - Certified in Cybersecurity

Version: DEMO

QUESTION 1
An entity that acts to exploit a target organization's system vulnerabilities is a:

A. Threat
B. Threat Vector
C. Threat Actor
D. Attacker

Answer: C
Explanation:
A Threat Actor is defined as an individual or a group posing a threat (according to NIST SP 800-150 under Threat Actor). A Threat Vector is a means by which a Threat Actor gains access to systems (for example: phishing, trojans, baiting, etc.). An Attacker is always an individual, but a Threat Actor can be either a group or an entity. A Threat is a circumstance or event that can adversely impact organizational operations that a Threat Actor can potentially explore through a Threat Vector.

QUESTION 2
Security posters are an element PRIMARILY employed in: ()

A. Business Continuity Plans
B. Physical Security Controls
C. Incident Response Plans
D. Security Awareness

Answer: D
Explanation:
Security posters are used to raise the awareness of employees regarding security threats, and thus are primarily employed in Security Awareness (see ISC2 Study Guide, chapter 5, module 4).

QUESTION 3
A best practice of patch management is to:

A. Apply patches according to the vendor's reputation
B. Apply patches every Wednesday
C. Test patches before applying them
D. Apply all patches as quickly as possible

Answer: C
Explanation:
Patches sometimes disrupt a system's configurations and stability. One of the main challenges for security professionals is to ensure that patches are deployed as quickly as possible, while simultaneously ensuring the stability of running systems. To prevent flawed patches from negatively affecting running systems, it is good practice to test patches in a designated qualification environment before applying them to production systems (see ISC2 Study Guide, chapter 5, module 2 under Configuration Management Overview). Applying patches as quickly as possible is not a good practice. The vendor's reputation can be useful to know, but is not in itself sufficient to qualify the patch. Applying patches on fixed days also does not guarantee the stability of functioning systems after the patch is applied.

QUESTION 4
Which of the following is NOT a social engineering technique? ()

A. Pretexting
B. Quid pro quo
C. Segregation
D. Baiting

Answer: C
Explanation:
In cybersecurity, 'segregation', or 'segregation of duties' (SoD), is a security principle designed to prevent fraud or error by dividing tasks among multiple persons.It is an administrative control that reduces the risk of potential errors or fraud from a single person having control over all aspects of a critical process. The remaining options are valid social engineering techniques. Baiting is a social engineering attack in which a scammer uses a false promise to lure a victim. Pretexting is a social engineering technique that manipulates victims into revealing information. Quid pro quo is a social engineering attack (technically a combination of baiting and pretexting) that promises users a benefit in exchange for information (that can later be used to gain control of a user's account or sensitive information).

QUESTION 5
Governments can impose financial penalties as a consequence of breaking a:

A. Regulation
B. Policy
C. Procedure
D. Standard

Answer: A
Explanation:
Standards are created by governing or professional bodies (not by governments themselves). Policies and procedures are created by organizations, and are therefore not subject to financial penalties (see ISC2 Study Guide Chapter 1, Module 4)

QUESTION 6
Malicious emails that aim to attack company executives are an example of:

A. Whaling
B. Trojans
C. Phishing
D. Rootkits

Answer: A
Explanation:
Phishing is a digital social engineering attack that uses authentic-looking (but counterfeit) e-mail messages to request information from users, or to get them to unknowingly execute an action that will make way for the attacker. Whaling attacks are phishing attacks that target high-ranking members of organizations. After gaining root-level access to a host, rootkits are used by an attacker to conceal malicious activities while keeping root-level access. Trojans are a type of software that appears legitimate but has hidden malicious functions that evade security mechanisms.

QUESTION 7
Which of these is the PRIMARY objective of a Disaster Recovery Plan?

A. Outline a safe escape procedure for the organization's personnel
B. Maintain crucial company operations in the event of a disaster
C. Restore company operation to the last-known reliable operation state
D. Communicate to the responsible entities the damage caused to operations in the event of a disaster

Answer: C
Explanation:
A Disaster Recovery Plan (DRP) is a plan for processing and restoring operations in the event of a significant hardware or software failure, or of the destruction of the organization's facilities. The primary goal of a DRP is to restore the business to the last-known reliable state of operations (see Chapter 2 ISC2 Study Guide, module 4, under The Goal of Disaster Recovery). Maintaining crucial operations is the goal of the Business Continuity Plan (BCP). The remaining options may be included in a DRP, but are not its primary objective.

QUESTION 8
Which of the following is NOT a protocol of the OSI Level 3?

A. IGMP
B. IP
C. SNMP
D. ICMP

Answer: C
Explanation:
Internet Protocol (IP) is known to be a level 3 protocol. Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP) are also level 3 protocols. Simple Network Management Protocol (SNMP) is a protocol used to configure and monitor devices attached to networks. It is an application-level protocol (level 7), and therefore the only option that is not from level 3.

QUESTION 9
Which type of attack attempts to trick the user into revealing personal information by sending a fraudulent message?

A. Phishing
B. Denials of Service
C. Cross-Site Scripting
D. Trojans

Answer: A
Explanation:
A phishing attack emails a fraudulent message to trick the recipient into disclosing sensitive information to the attacker. A Cross-Site Scripting attack tries to execute code on another website. Trojans are software that appear legitimate, but that have hidden malicious functions. Trojans may be sent in a message, but are not the message themselves. A denial of service

attack (DoS) consists in compromising the availability of a system or service through a malicious overload of requests, which causes the activation of safety mechanisms that delay or limit the availability of that system or service.

QUESTION 10
Which of the following documents contains elements that are NOT mandatory?

A. Policies
B. Guidelines
C. Regulations
D. Procedures

Answer: B
Explanation:
Only guidelines contain elements that may not be mandatory. Compliance with policies, procedures and regulations is mandatory (see ISC2 Study Guide Chapter 1, Module 4).

QUESTION 11
The process of verifying or proving the user's identification is known as:

A. Integrity
B. Authorization
C. Authentication
D. Confidentiality

Answer: C
Explanation:
Authentication is the verification of the identity of a user, process or device, as a prerequisite to allowing access to the resources in a given system. In contrast, authorization refers to the permission granted to users, processes or devices to access specific assets. Confidentiality and integrity are properties of information and systems, not processes.

QUESTION 12
Which of these is NOT a change management component?

A. Approval
B. Rollback
C. Governance
D. RFC

Answer: C
Explanation:
All significant change management practices address typical core activities: Request For Change (RFC), Approval, and Rollback (see ISC2 Study Guide, chapter 5, module 3). Governance is not one of these practices.

QUESTION 13
Which type of key can be used to both encrypt and decrypt the same message?

A. A symmetric key
B. A private key
C. An asymmetric key
D. A public key

Answer: A
Explanation:
Symmetric-key algorithms are a class of cryptographic algorithms that use a single key for both encrypting and decrypting of data. Asymmetric cryptography uses pairs of related keys: the public and the corresponding private keys. A message encrypted with the public key can only be decrypted by its corresponding private key, and vice versa. The term 'asymmetric key' is not applicable here.

QUESTION 14
Which of these has the PRIMARY objective of identifying and prioritizing critical business processes?

A. Business Continuity Plan
B. Business Impact Plan
C. Business Impact Analysis
D. Disaster Recovery Plan

Answer: C
Explanation:
The term 'Business Impact Plan' does not exist. A Business Impact Analysis (BIA) is a technique for analyzing how disruptions can affect an organization, and determines the criticality of all business activities and associated resources. A Business Continuity Plan (BCP) is a pre-determined set of instructions describing how the mission/business processes of an organization will be sustained during and after a significant disruption. A Disaster Recovery Plan is a written plan for recovering information systems in response to a major failure or disaster.

QUESTION 15
How many layers does the OSI model have?

A. 7
B. 4
C. 5
D. 6

Answer: A
Explanation:
The OSI model organizes communicating systems according to 7 layers: Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer (see Chapter 4 - Module 1 under Open Systems Interconnection).

QUESTION 16
Which type of attack embeds malicious payload inside a reputable or trusted software?

A. Rootkits
B. Phishing

C. Trojans
D. Cross-Site Scripting

Answer: C
Explanation:
Trojans are a type of software that appears legitimate but has hidden malicious functions that evade security mechanisms, typically by exploiting legitimate authorizations of the user that invokes the program. Rootkits try to maintain privilege-level
access while concealing malicious activity. They often replace system files, so they are activated when the system is restarted. Trojans often install Rootkits, but Rootkits are not the Trojans themselves). Phishing typically tries to redirect the user to another website. Cross-site scripting attempts to inject malicious executable code into a website.

QUESTION 17
A security safeguard is the same as a:

A. Security control
B. Safety control
C. Privacy control
D. Security principle

Answer: A
Explanation:
Security safeguards are approved security measures taken to protect computational resources by eliminating or reducing the risk to a system. These can be measures like hardware and software mechanisms, policies, procedures, and physical controls (see NIST SP 800-28 Version 2, under safeguard). This definition matches the definition of security control as the means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature (see NIST SP 800-160 Vol. 2 Rev. 1 under control).

QUESTION 18
Which of the following properties is NOT guaranteed by Digital Signatures?

A. Integrity
B. Confidentiality
C. Non-repudiation
D. Authentication

Answer: B
Explanation:
The correct answer is
B. A digital signature is the result of a cryptographic transformation of data which is useful for providing: data origin authentication, data integrity, and non-repudiation of the signer (see NIST SP 800-12 Rev. 1 under Digital Signature). However, digital signatures cannot guarantee confidentiality (i.e. the property of data or information not being made available or disclosed).

QUESTION 19
According to the canon "Provide diligent and competent service to principals", (ISC)?professionals are to:

A. Avoid apparent or actual conflicts of interest
B. Promote the understanding and acceptance of prudent information security measures
C. Take care not to tarnish the reputation of other professionals through malice or indifference
D. Treat all members fairly and,when resolving conflicts, consider public safety and duties to principals, individuals and the profession, in that order

Answer: A
Explanation:
The direction for applying the ethical principles of ISC2 states that avoiding conflicts of interest or the appearance thereof is a consequence of providing diligent and competent service to principals (see https://resources.infosecinstitute.com/certification/the-isc2-code-of-ethics-a-binding-requirement-for-certification/). The other options are consequences of the remaining three ethical principles.

QUESTION 20
Which of the following is an example of 2FA?

A. Keys
B. Passwords
C. Badges
D. One-Time passwords (OTA)

Answer: D
Explanation:
One-time passwords are typically generated by a device (i.e. "something you have") and are required in addition to the actual main password (i.e. "something you know"). Badges, keys and passwords with no other overlapping authentication controls are considered single-factor (and thus are not 2FA).

QUESTION 21
Which of the following principles aims primarily at fraud detection?

A. Defense in Depth
B. Separation of Duties
C. Least Privilege
D. Privileged Accounts

Answer: B
Explanation:
According to the principle of Separation of Duties, operations on objects are to be segmented (often referred to as 'transactions'), requiring distinct users and authorizations. The involvement of multiple users guarantees that no single user can perpetrate and conceal errors or fraud in their duties. To the extent that users have to review the work of other users, Separation of Duties can also be considered a mechanism of fraud detection (see ISC2 Study Guide Chapter 1, Module 3). The principle of Least Privilege states that subjects should be given only those privileges required to complete their specific tasks. The principle of Privileged Accounts refers to the existence of accounts with permissions beyond those of regular users. Finally, the principle of Defense in Depth endorses the use of multiple layers of security for holistic protection.

QUESTION 22

Which cloud deployment model is suited to companies with similar needs and concerns?

A. Private cloud
B. Community cloud
C. Hybrid cloud
D. Multi-tenant

Answer: B
Explanation:
The correct answer is
B. Community cloud deployment models are where several organizations with similar needs and concerns (technological or regulatory) share the infrastructure and resources of a cloud environment. This model is attractive
because it is cost-effective while addressing the specific requirements of the participating organizations. A private cloud is a cloud computing model where the cloud infrastructure is dedicated to a single organization (and never shared with others). A hybrid cloud is a model that combines (i.e. orchestrates) on-premises infrastructure, private cloud services, and a public cloud to handle storage and service. Finally, multitenancy refers to a cloud architecture where multiple cloud tenants (organizations or users) share the same computing resources. Yet, while resources are shared, each tenant's data is isolated and remains invisible to other tenants.

QUESTION 23
Which of the following is NOT a possible model for an Incident Response Team (IRT)?

A. Hybrid
B. Pre-existing
C. Leveraged
D. Dedicated

Answer: B
Explanation:
The three possible models for incident response are Leveraged, Dedicated, and Hybrid (see the ISC2 Study Guide, Chapter 2, Module 1, under Chapter Takeaways). The term 'Pre-existing' is not a valid model for an IRT.

QUESTION 24
A web server that accepts requests from external clients should be placed in which network?

A. VPN
B. Internal Network
C. Intranet
D. DMZ

Answer: D
Explanation:
In Cybersecurity, a DMZ (demilitarized zone) is a physical or logical subnetwork that contains and exposes external-facing services (such as web services). An Internal Network is an organization-controlled network that is isolated from external access. An Intranet is itself an internal network that supports similar protocols and services to the Internet, but only for the organization's internal use. A Virtual Private Network (VPN) creates a secure tunnel between endpoints (whether between networks, or between networks and devices), allowing traffic to travel through a public

network and creating the illusion that endpoints are connected through a dedicated private connection.

QUESTION 25
A device found not to comply with the security baseline should be:

A. Marked as potentially vulnerable and placed in a quarantine area
B. Disabled or separated into a quarantine area until a virus scan can be run
C. Placed in a demilitarized zone (DMZ) until it can be reviewed and updated
D. Disabled or isolated into a quarantine area until it can be checked and updated

Answer: D
Explanation:
Security baselines are used to guarantee that network devices, software, hardware and endpoints are configured consistently. Baselines ensure that all such devices comply with the security baseline set by the organization. Whenever a device is found not compliant with the security baseline, it may be disabled or isolated into a quarantine area until it can be checked and updated (see ISC2 Study Guide, chapter 5, module 2, under Configuration Management Overview). A DMZ is a protected boundary network between external and internal networks. Systems accessible directly from the Internet are permanently connected in this network, where they are protected by a firewall; however, a DMZ is not a quarantine area used to temporarily isolate devices.

QUESTION 26
What is the consequence of a Denial of Service attack?

A. Increase in the availability of resources
B. Malware Infection
C. Remote control of a device
D. Exhaustion of device resources

Answer: D
Explanation:
A denial of service attack (DoS) consists in a malicious overload of requests which will eventually lead to the exhaustion of resources, rendering the service unavailable, as well as causing the activation of safety mechanisms that delay or limit the availability of that system or service. This type of attack seeks to compromise service availability, but not to control a device nor to install malware.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**