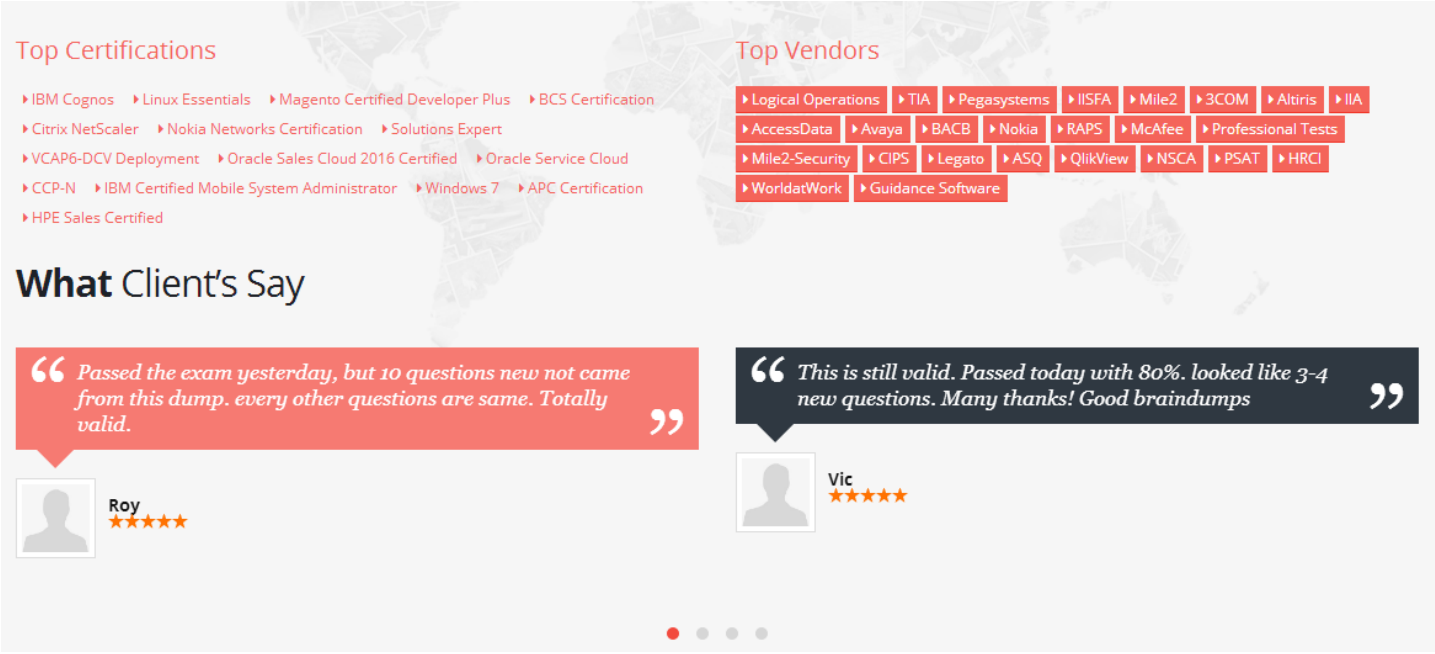
Lead2passExam



http://www.lead2passexam.com/

Available Exam Cram and Valid Dumps - Lead2Pass Exam

Exam : **CC**

Title : Certified in Cybersecurity (CC)

Vendor : ISC

Version : DEMO

NO.1 Which of the following properties is NOT guaranteed by digital signatures?
A. Authentication
B. Confidentiality
C. Non-repudiation
D. Integrity
Answer: B
Explanation:
Digital signatures provideauthentication,integrity, andnon-repudiation, but they donot provide confidentiality.
A digital signature verifies who sent the message and ensures it was not altered, but the content remains readable unless encryption is also applied.
Confidentiality requires encryption, typically using symmetric or asymmetric cryptography. Digital signatures are often combined with encryption (such as in TLS or secure email), but by themselves they do not hide message contents.

NO.2 What security feature is used in HTTPS?
A. IPSec
B. SSH
C. ICMP
D. SSL/TLS
Answer: D
Explanation:
HTTPS uses SSL/TLS to provide encryption, authentication, and integrity for web communications.

NO.3 Created by switches to logically segment a network without changing physical topology:
A. LAN
B. WAN
C. VLAN
D. MAN
Answer: C
Explanation:
VLANslogically separate networks at Layer 2 while sharing the same physical infrastructure.

NO.4 A logical group of workstations, servers, and network devices that appear to be on the same LAN despite their geographical distribution.
A. LAN
B. VPN
C. WLAN
D. VLAN
Answer: D
Explanation:
A Virtual Local Area Network (VLAN) is a logical segmentation of network devices that allows systems to appear as though they are on the same local network, regardless of their physical location. VLANs operate at the Data Link layer (Layer 2) and use tagging (such as IEEE 802.1Q) to separate broadcast

domains logically.
VLANs improve security, performance, and manageability by isolating traffic between different groups of systems. Devices in the same VLAN can communicate as if they were on the same LAN, even if they are physically distributed across different switches or buildings.
LAN refers to a physical local network, VPN provides encrypted tunnels across networks, and WLAN refers to wireless LANs. Only VLANs provide logical grouping independent of geography.

NO.5 VLAN hopping belongs to which OSI layer?
A. Layer 3
B. Layer 4
C. Layer 7
D. Layer 2
Answer: D
Explanation:
VLAN hopping exploits weaknesses in Layer 2 switching mechanisms such as trunking and tagging.

NO.6 Ignoring a risk and continuing business operations is known as:
A. Risk acceptance
B. Risk mitigation
C. Risk avoidance
D. Risk transfer
Answer: A
Explanation:
Risk acceptance acknowledges the risk and chooses to proceed without additional controls, often due to cost or low impact.

NO.7 How often should an organization test its BCP?
A. Continually
B. Annually
C. Routinely
D. Daily
Answer: C
Explanation:
BCPs should be testedroutinely(e.g., tabletop, simulations) to ensure readiness and relevance.

NO.8 What are registered ports primarily used for?
A. Core TCP/IP protocols
B. Web servers
C. In-house applications
D. Vendor and proprietary applications
Answer: D
Explanation:
Registered ports (1024-49151) are typically assigned to vendor-specific or proprietary applications, such as database services.

NO.9 Faking the sender address of a transmission to gain illegal entry is called:
A. Phishing
B. ARP
C. Spoofing
D. All
Answer: C
Explanation:
Spoofing involves falsifying identity information (IP, MAC, email headers) to appear as a trusted source and bypass controls.

NO.10 What does Personally Identifiable Information (PII) pertain to?
A. Information about an individual's health status
B. Data about an individual that could be used to identify them
C. Trade secrets, research, business plans, and intellectual property
D. The importance assigned to information by its owner
Answer: B
Explanation:
Personally Identifiable Information (PII) refers to any data that can be used to identify a specific individual, either directly or indirectly. Examples include full name, Social Security number, date of birth, address, email address, phone number, and biometric identifiers.
PII is regulated by numerous laws and standards, including privacy regulations and data protection frameworks. Protecting PII is critical to prevent identity theft, fraud, and privacy violations.
Health information is a subset of sensitive data (often classified as PHI). Trade secrets and business data fall under intellectual property. Information classification levels describe value, not identity.
Security controls for PII typically include encryption, access control, monitoring, and data loss prevention mechanisms.

NO.11 Which is the first step in the risk management process?
A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment
Answer: C
Explanation:
Risk identification is the first step in the risk management process. Organizations must first identify assets, threats, and vulnerabilities before they can assess likelihood or impact. Without knowing what risks exist, meaningful assessment and mitigation are impossible.

NO.12 Which principle states that users should have access only to the specific data and resources needed to perform required tasks?
A. Zero Trust
B. Defense in Depth
C. Least Privilege

D. All

Answer: C

Explanation:

ThePrinciple of Least Privilegeensures users, applications, and systems have only the minimum permissions necessary to perform their duties. This reduces the attack surface and limits potential damage if credentials are compromised.

NO.13 Uses multiple types of access controls in layered fashion to avoid monolithic security:

A. DMZ

B. VLAN

C. Defense in Depth

D. VPN

Answer: C

Explanation:

Defense in Depth employs administrative, technical, and physical controls across multiple layers to reduce reliance on any single security mechanism. This approach increases resilience and detection capability.

NO.14 Malicious code that acts like a remotely controlled "robot" for an attacker.

A. Rootkit

B. Malware

C. Bot

D. Virus

Answer: C

Explanation:

Abotis malware that allows attackers to remotely control infected systems, often forming botnets used for DDoS attacks, spam, or credential theft.

NO.15 The Bell-LaPadula access control model is a form of:

A. RBAC

B. MAC

C. DAC

D. ABAC

Answer: B

Explanation:

Bell-LaPadula is a Mandatory Access Control (MAC) model focused on confidentiality. It uses security labels and clearances to enforce access rules such as "no read up, no write down."

NO.16 A method for risk analysis that is based on the assignment of a descriptor such as low, medium, or high.

A. Quantitative Risk Analysis

B. Risk Assessment

C. Risk Mitigation

D. Qualitative Risk Analysis

Answer: D
Explanation:
Qualitative risk analysis evaluates risk using descriptive categories such aslow,medium, andhighinstead of numerical values. This approach relies on expert judgment, experience, and contextual understanding rather than precise financial or statistical calculations. According to NIST SP 800-30, qualitative analysis is especially useful when numerical data is unavailable or when rapid risk prioritization is required.
Unlike quantitative risk analysis, which assigns monetary values and probabilities, qualitative analysis focuses on relative severity and likelihood. It is commonly used during early stages of risk management, policy development, and executive decision-making. While less precise, qualitative risk analysis is easier to communicate to stakeholders and helps organizations focus resources on the most critical risks.

NO.17 A company network experiences a sudden flood of network packets that causes major slowdown in Internet traffic. What type of event is this?
A. Security incident
B. Natural disaster
C. Exploit
D. Adverse event
Answer: D
Explanation:
A sudden flood of network packets causing degraded performance is best classified as anadverse event. An adverse event is any occurrence that negatively affects system performance, availability, or operations but may not yet meet the threshold of a confirmed security incident. According to NIST definitions, events such as traffic spikes, system slowdowns, or anomalous behavior are initially treated as adverse events until further analysis confirms malicious intent.
If investigation later confirms the flood was caused by a deliberate denial-of-service attack, the classification may escalate to asecurity incident. However, without confirmation of intent or compromise, adverse event is the most accurate term.

NO.18 Which security control is most commonly used to prevent data breaches?
A. Physical control
B. Logical control
C. Administrative control
D. RBAC
Answer: B
Explanation:
Logical (technical) controls such as encryption, access controls, DLP, and firewalls directly prevent unauthorized data access and exfiltration.

NO.19 Which allows extremely granular restrictions down to individual machines or users?
A. DMZ
B. Microsegmentation
C. VLAN
D. NAC

Answer: B
Explanation:
Microsegmentation enables fine-grained, software-defined security controls, limiting lateral movement within networks.

NO.20 The magnitude of harm expected from unauthorized disclosure, modification, destruction, or loss of information is known as:
A. Threat
B. Vulnerability
C. Impact
D. Likelihood
Answer: C
Explanation:
Impact measures the severity of consequences if a security event occurs. It is a key component of risk calculations along with likelihood.

NO.21 Example of dynamic authorization:
A. DAC
B. RBAC
C. MAC
D. ABAC
Answer: D
Explanation:
Attribute-Based Access Control (ABAC) is considered a dynamic authorization model because access decisions are made in real time based on attributes of the user, resource, action, and environment. These attributes can include time of day, device type, location, data sensitivity, and user role.
Unlike RBAC or MAC, which rely on static roles or labels, ABAC evaluates policies dynamically using a policy decision point (PDP). This makes ABAC ideal for modern cloud, zero trust, and highly distributed environments.
DAC allows owners to grant permissions, RBAC uses predefined roles, and MAC relies on fixed security labels. ABAC provides the most flexible and context-aware authorization.

NO.22 Which activity is often associated with Disaster Recovery efforts?
A. Running anti-malware
B. Vulnerability scanning
C. Zero-day exploits
D. Employees returning to the primary production location
Answer: D
Explanation:
Disaster Recovery includes restoring systems and returning operations to normal, which may involve staff moving back to the primary site after temporary relocation.

NO.23 A set of rules that everyone must comply with and that usually carry monetary penalties for noncompliance are:

A. Standards
B. Policies
C. Procedures
D. Laws or regulations
Answer: D
Explanation:
Laws and regulations are legally enforceable and can impose fines or penalties. Standards and policies are not legally binding unless mandated by regulation.

NO.24 What goal of security is enhanced by a strong business continuity program?
A. Non-repudiation
B. Availability
C. Confidentiality
D. Integrity
Answer: B
Explanation:
Availability is the primary security goal enhanced by a strong business continuity program. Business continuity planning focuses on ensuring that critical systems, services, and operations remain accessible during and after disruptive events such as cyberattacks, natural disasters, or system failures.
Availability is one of the three pillars of the CIA triad and ensures that authorized users can access information and systems when needed. Business continuity strategies include redundancy, failover systems, backups, alternate processing sites, and disaster recovery plans.
While confidentiality and integrity are important, business continuity is primarily concerned with minimizing downtime and maintaining operational resilience. Non-repudiation relates to accountability and is not a continuity objective.
Frameworks such as NIST SP 800-34 and ISO/IEC 22301 emphasize availability as the core outcome of effective business continuity and disaster recovery planning.

NO.25 XenServer, LVM, Hyper-V, and ESXi are:
A. Type 2 hypervisors
B. Type 1 hypervisors
C. Both
D. None
Answer: B
Explanation:
These areType 1 (bare-metal) hypervisors, running directly on hardware without a host operating system, offering higher performance and security.

NO.26 Which technology should be implemented to increase the work effort required for buffer overflow attacks?
A. Address Space Layout Randomization
B. Memory induction application
C. Input memory isolation

D. Read-only memory integrity checks

Answer: A

Explanation:

Address Space Layout Randomization (ASLR) randomizes the memory locations used by applications, making it significantly harder for attackers to predict where malicious payloads should be placed during buffer overflow attacks.

Buffer overflow exploits rely on predictable memory layouts. ASLR disrupts this predictability, increasing attacker effort and reducing exploit reliability.

The other options are either non-standard terms or unrelated to buffer overflow mitigation. ASLR is widely used in modern operating systems and is a key defensive control recommended by secure coding and system hardening guidelines.

ASLR does not eliminate vulnerabilities but raises the attack complexity, which is a core defensive strategy.

NO.27 How do IT professionals differentiate between IT problems and security incidents?

A. Medical assistance

B. Evidence collection only

C. Specialized incident response training

D. Lessons learned participation

Answer: C

Explanation:

Incident response training enables professionals to recognize malicious activity versus routine IT failures and respond appropriately.

NO.28 Which is an example of a deterrent control?

A. Biometric

B. Guard dog

C. Encryption

D. Turnstile

Answer: B

Explanation:

A guard dog deters unauthorized access by increasing perceived risk. Deterrent controls discourage attacks before they occur.

NO.29 An IP network protocol standardized by the IETF through RFC 792 to determine if a host is available is:

A. IP

B. ICMP

C. IGMP

D. HTTP

Answer: B

Explanation:

ICMP is used for network diagnostics, including ping operations that test host availability. RFC 792 defines ICMP behavior.

NO.30 To avoid bodily injury claims, a company decides not to offer high-risk services. This is an example of:
A. Risk Acceptance
B. Risk Assessment
C. Risk Avoidance
D. Risk Control
Answer: C
Explanation:
Risk Avoidanceeliminates risk by discontinuing activities that expose the organization to unacceptable threats.

NO.31 A set of instructions to detect, respond to, and recover from security incidents is a:
A. BCP
B. IRP
C. DRP
D. None
Answer: B
Explanation:
An Incident Response Plan (IRP) defines procedures for managing and mitigating security incidents.

NO.32 Which OSI layer associates MAC addresses with network devices?
A. Physical layer
B. Network layer
C. Data Link layer
D. Transport layer
Answer: C
Explanation:
The Data Link layer (Layer 2) handles MAC addressing and frame delivery within local networks.

NO.33 The purpose of risk identification is:
A. Employees at all levels help identify risks
B. Identify risks to communicate clearly
C. Identify risks to protect against them
D. All
Answer: D
Explanation:
Risk identification is a collaborative process that enables awareness, communication, and protection against threats.

NO.34 When the ISC2 mail server sends mail to other mail servers, it becomes a -?
A. SMTP Server
B. SMTP Peer
C. SMTP Master

D. SMTP Client

Answer: D

Explanation:

When a mail server sends email to another mail server, it acts as anSMTP client. In the Simple Mail Transfer Protocol (SMTP), roles are defined by behavior, not by the system's primary function.

The sending system initiates the connection and issues SMTP commands, which makes it the client for that transaction. The receiving mail server listens for incoming connections and acts as the SMTP server.

Mail servers routinely switch roles depending on the direction of communication. A single system may act as an SMTP server when receiving mail and as an SMTP client when sending mail.

Understanding SMTP roles is important for configuring mail security controls such as firewalls, TLS enforcement, spam filtering, and authentication. Security professionals must recognize that "client" and

"server" are session-based roles, not permanent system identities.

NO.35 What is the recommended fire suppression system for server rooms?

A. Foam-based

B. Water-based

C. Powder-based

D. Clean-agent gas systems (e.g., FM-200 / Inergen)

Answer: D

Explanation:

Clean-agent fire suppression systems such as FM-200 and Inergen are recommended for server rooms because they suppress fires without damaging electronic equipment. Water, foam, and powder systems can destroy hardware and cause prolonged outages.

Clean agents extinguish fires by reducing heat or oxygen levels while remaining safe for occupied spaces.

NIST and data center best practices strongly recommend clean-agent systems for mission-critical environments.