



ISC2

Exam Questions CC

Certified in Cybersecurity (CC)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Structured way to align IT with business goals while managing risks and meeting all industry and government regulations

- A. GRC
- B. Policies
- C. Law
- D. Stanford

Answer: A

NEW QUESTION 2

What are registered port used for

- A. Common protocols at the core of TCP/IP model
- B. Used for web servers
- C. Used for in housed or opensource applications
- D. Proprietary applications from vendors and developpe

Answer: D

NEW QUESTION 3

A chief information security officer (CISO) at a large organization documented a policy that establishes the acceptable use of cloud environments for all staff. This is an example of

- A. Technical control
- B. Physical control
- C. Cloud control
- D. Management/Administrative control

Answer: D

NEW QUESTION 4

Configuration settings or parameters stored as data, managed through a software graphical user interface (GUI) is

- A. Logical access control
- B. Physical access control
- C. Administrative Access control

Answer: A

NEW QUESTION 5

A set of security controls or system settings used to ensure uniformity of configuration through the IT environment?

- A. Patches
- B. Inventory
- C. Baseline
- D. Policy

Answer: C

NEW QUESTION 6

Which term describes a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network?

- A. Zero Trust
- B. DMZ
- C. VPN
- D. None of the Above

Answer: C

NEW QUESTION 7

A hacker gains access to a compony network and begins to intercept network traffic in order to steal login credentials which OSI layer is being attacked

- A. Data Link layer
- B. Physical layer
- C. Network Layer
- D. Application laver

Answer: D

NEW QUESTION 8

System capabilities designed to detect and prevent the unauthorized use and transmission of information.

- A. SOC
- B. SIEM solutions
- C. Data Loss Prevention
- D. Cryptography

Answer: C

NEW QUESTION 9

A _____ creates an encrypted tunnel to protect your personal data and communications

- A. HTTPS
- B. VPN
- C. Anti-virus
- D. IDS

Answer: B

NEW QUESTION 10

Which of the following is a systematic approach to protecting against cyber threats that involves a continuous cycle of identifying, assessing and prioritizing risks and implementing measures to reduce or eliminate those risks?

- A. Security Assessment
- B. Incident response
- C. Penetration testing
- D. Risk Management

Answer: D

NEW QUESTION 10

What is the range of well known ports

- A. 0 - 1023
- B. 1023-49151
- C. 49152 - 65535
- D. None

Answer: A

NEW QUESTION 15

Faking the sending address of a transmission to gain illegal entry into a secure system.

- A. Phishing
- B. ARP
- C. Spoofing
- D. ALL

Answer: C

NEW QUESTION 16

Port forwarding is also known as

- A. Port mapping
- B. Tunneling
- C. Punch through
- D. ALL

Answer: D

NEW QUESTION 21

COVID-19 is one of the perfect example of a situation, where a _____ plan is enacted to sustain the business

- A. IRP
- B. DRP
- C. BCP
- D. ALL

Answer: C

NEW QUESTION 26

Is a way to prevent unwanted devices from connecting to a network.

- A. DMZ
- B. VPN
- C. VLAN
- D. NAC

Answer: D

NEW QUESTION 29

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

- A. DDOS
- B. Authentication
- C. Authentication
- D. Availability

Answer: A

NEW QUESTION 31

Which version of TLS is considered to be the most secure and recommended for use?

- A. TLS 1.0
- B. TLS 1.1
- C. TLS 1.2
- D. TLS 1.3

Answer: D

NEW QUESTION 35

A tool used to inspect outbound traffic to reduce threats

- A. Anti-malware
- B. NIDC
- C. DLP
- D. Firewall

Answer: C

NEW QUESTION 40

A scammer will attempt to make a malicious website look exactly like a legitimate one that the victim knows and trusts

- A. DOS
- B. Virus
- C. Spoofing
- D. Phishing

Answer: C

NEW QUESTION 43

Difference between Sniffing and Snooping

- A. Sniffing is the process of intercepting and collecting network traffic as it passes over a digital network
- B. Spoofing is the act of disguising a communication from an unknown source as being trustworthy.
- C. Snooping is the process of intercepting and collecting network traffic as it passes over a digital network
- D. Sniffing is the act of disguising a communication from an unknown source as being trustworthy.
- E. Both are same
- F. Sniffing is not thread and snooping is a thread

Answer: A

NEW QUESTION 47

What does Criticality represents?

- A. The need for consultation with the involved business ensure critical systems are identified and available
- B. The importance an organization gives to data or an information system in performing its operations or achieving its mission
- C. The need for security professional to ensure the appropriate levels of availability are provided
- D. All of the above

Answer: B

NEW QUESTION 49

Which component of the incident response plan involves identifying critical data and systems?

- A. Detection and Analysis
- B. Preparation
- C. Containment
- D. Eradication

Answer: B

NEW QUESTION 51

A company needs to protect its confidential data from unauthorized access which logical control is best suited for this scenario

- A. Encryption
- B. Firewall
- C. Antivirus
- D. Hashing

Answer: A

NEW QUESTION 54

Is an integrated platform and graphical tool for performing security testing of web applications.

- A. Burp suite
- B. Wireshark C Fiddler
- C. ZenMap

Answer: A

NEW QUESTION 55

When is the Business Continuity Plan Enacted?

- A. When there is a event
- B. When there is a incident
- C. When there is a loss of business operations
- D. When there is a natural disaster

Answer: C

NEW QUESTION 56

Which of the following uses registered port

- A. HTTP
- B. SMB
- C. TCP
- D. MS Sql server

Answer: D

NEW QUESTION 61

Which aspect of cybersecurity is MOST impacted by Distributed Denial of Service (DDoS) attacks?

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

Answer: C

NEW QUESTION 63

Which of the following is not a source of redundant power

- A. Generator
- B. Utility
- C. UPS
- D. HVAC

Answer: D

NEW QUESTION 66

Which of the following security controls is designed to prevent unauthorized access to sensitive information by ensuring that it is only accessible to authorized users?

- A. Encryption
- B. Firewall
- C. Antivirus
- D. Access control

Answer: D

NEW QUESTION 69

What is a threat in the context of cybersecurity

- A. An inherent weakness or flaw in a system
- B. Something in need of protection

- C. The means by which a threat actor carries out their objectives
- D. A person or thing that takes action to exploit a target organizations system vulnerabilities

Answer: D

NEW QUESTION 74

What does a breach refer to in the context of cybersecurity

- A. An unauthorized access to a system or system recours
- B. Any observable occurance in a network or system
- C. A deiberate security incident
- D. A previously know system vulnerablity

Answer: A

NEW QUESTION 75

Who should participate in creating a BCP

- A. Only members from the IT department
- B. Only members from the management team
- C. Members from across the organization
- D. Only members from the finanace department

Answer: C

NEW QUESTION 76

A company network has been infected with malware and all its servers are down. What is the first step that the Disaster Recovery team should take to restore the systems?

- A. Disconnect the affected systems from the network
- B. Conduct a risk assessment of determine the extent of the damage
- C. Restore data from backup systems
- D. Contact the enforcement to investigate the cyberattack

Answer: A

NEW QUESTION 79

Which type of encryption uses only one shared key to encrypt and decrypt?

- A. Public key
- B. Asymmetric
- C. Symmetric
- D. TCB key

Answer: C

NEW QUESTION 84

provide integrity services that allow a recipient to verify that a message has not been altered.

- A. Hashing
- B. encryption
- C. decryption
- D. encoding

Answer: A

NEW QUESTION 87

Modern solutions try to provide a more holistic approach detecting rootkits, ransomware and spyware.

- A. Antivirus
- B. IDS
- C. IPS
- D. Anti Malware

Answer: D

NEW QUESTION 90

Which phase of the access control process(AAA) does a user prove his/her identity?

- A. Authentication
- B. Authorization
- C. Identification
- D. Accounting

Answer: A

NEW QUESTION 94

What is the end goal of DRP

- A. All System backup restored
- B. DR site activated
- C. Shifting the Infrastructure to new place
- D. Business restored to full last-known reliable operations.

Answer: D

NEW QUESTION 95

How does IPSec protect against replay attacks

- A. By using sequence numbers
- B. By limiting access to the network
- C. By using digital signatures
- D. By encryption all network traffic

Answer: A

NEW QUESTION 97

The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards

- A. ISO
- B. NIST
- C. IETF
- D. GDPR

Answer: C

NEW QUESTION 100

A portion of the organization's network that interfaces directly with the outside world; typically, this exposed area has more security controls and restrictions than the rest of the internal IT environment.

- A. Virtual private network (VPN)
- B. Virtual local area network (VLAN)
- C. Zero Trust
- D. Demilitarized zone (DMZ)

Answer: D

NEW QUESTION 101

How often should an organization test its business continuity plan

- A. Continually
- B. Annually
- C. Routinely
- D. Daily

Answer: C

NEW QUESTION 106

What is the first step in incident response planning

- A. Develop a policy approved by management
- B. Identify critical data and systems
- C. Train staff on incident response
- D. implement an incident response team

Answer: A

NEW QUESTION 109

Exhibit.

OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

IPSec works in which layer of OSI Model

- A. Layer 2
- B. Layer 5
- C. Layer 3
- D. Layer 7

Answer: C

NEW QUESTION 114

Which of the following is NOT one of the three main components of a sql database?

- A. Views
- B. Schemas
- C. Tables
- D. Object-oriented interfaces

Answer: D

NEW QUESTION 118

Which penetration testing technique requires the team to do the MOST work and effort?

- A. White box
- B. Blue box
- C. Gray box
- D. Black box

Answer: D

NEW QUESTION 123

DevOps team has updated the application source code, Tom has discovered that many unauthorized changes have been made. What is the BEST control Tom can implement to prevent a recurrence of this problem?

- A. Backup
- B. File labels
- C. Security audit
- D. Hashing

Answer: D

NEW QUESTION 126

_____ are virtual separations within a switch and are used mainly to limit broadcast traffic

- A. LAN
- B. WAN
- C. VLAN
- D. MAN

Answer: C

NEW QUESTION 128

A company wants to ensure that its employees cannot bring unauthorized electronic devices into the workspace which physical control is best suited for this

- A. Metal Detectors
- B. Security gaurds
- C. RFID scanners
- D. Baggage X-ray machinces

Answer: A

NEW QUESTION 130

Which of the following best describes the type of technology the team should implement to increase the work effort of buffer overflow attacks?

- A. Address space layout randomization
- B. Memory induction application
- C. Input memory isolation
- D. Read-only memory integrity checks

Answer: A

NEW QUESTION 135

Which of these is WEAKEST form of authentication we can implement?

- A. Something you know
- B. Something you are
- C. Something you have
- D. Biometric authentications

Answer: A

NEW QUESTION 139

Which type of authentication is something which you

- A. Type1
- B. Type 2
- C. Type 3
- D. Type 4

Answer: C

NEW QUESTION 144

Why is the recovery of IT often crucial to the recovery and sustainment of business operations

- A. IT is not important to business operation
- B. IT often the cause for the disaster
- C. IT can be easily recovers without any impact of business operations
- D. Many business rely heavily on IT for their operations

Answer: D

NEW QUESTION 148

Networks are often micro segmented networks, with firewalls at nearly every connecting point

- A. DMZ
- B. VPN
- C. VLAN
- D. Zero Trust

Answer: A

NEW QUESTION 150

Your organization is concerned about network security and wants to prevent unauthorized access to its resources by implementing a security model where the network has not trusted space what type of security model is this

- A. Zero trust
- B. Trusted computing
- C. Trusted platform modelus
- D. Trusted execution environment

Answer: A

NEW QUESTION 154

Which security control mostly used to prevent data breach

- A. Physical control
- B. Logical Control
- C. Administrative Control
- D. RBAC

Answer: B

NEW QUESTION 155

An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.

- A. IP
- B. ICMP
- C. IGMP
- D. HTTP

Answer: B

NEW QUESTION 160

What is the first component the new security engineer should learn about in the incident response plan?

- A. Detection and analysis
- B. Preparation
- C. Containment
- D. Eradication

Answer: B

NEW QUESTION 164

Which type of fire suppression system is more friendly to electronics

- A. Carbon di Oxide based
- B. Chemical based
- C. Water based
- D. Foam based

Answer: A

NEW QUESTION 165

Which protocol would be most suitable to fulfill the secure communication requirements between clients and the server for a company deploying a new application?

- A. FTP
- B. HTTP
- C. HTTPS
- D. SMTP

Answer: C

NEW QUESTION 166

Which of the following protocols is a secure alternative to using telnet?

- A. SSH
- B. HTTPS
- C. SFTP
- D. LDAPS

Answer: B

NEW QUESTION 170

What is the purpose of multi-factor authentication (MFA) in IAM?

- A. To simplify user access
- B. To eliminate the need for authentication
- C. To add an additional layer of security by requiring multiple forms of verification
- D. To grant unrestricted access to all users

Answer: C

NEW QUESTION 175

A set of instructions to help IT staff detect, respond to, and recover from network security incidents?

- A. BCP
- B. IRP
- C. DRP
- D. None

Answer: B

NEW QUESTION 180

organization experiences a security event that potentially jeopardizes the confidentiality, integrity or availability of its information system. What term best describes this situation?

- A. Breach
- B. Event
- C. Incident
- D. Exploit

Answer: C

NEW QUESTION 185

An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant

- A. Eavesdropping Attack
- B. CSRF
- C. XSS
- D. ARP Spoofing

Answer: A

NEW QUESTION 189

Which type of control is used to restore systems or processes to their normal state after an attack has occurred

- A. Compensatory Control
- B. Recovery Control
- C. Detective Control
- D. Corrective Control

Answer: D

NEW QUESTION 193

Which of the following documents identifies the principles and rules governing an organization's protection of information systems and data

- A. Procudure
- B. Guideline
- C. Policy
- D. Standard

Answer: C

NEW QUESTION 194

What are the primary responsibilities of a computer incident response team (CIRT) during an incident?

- A. To determine the difference between minor and major incident
- B. To troubleshoot network and system issues
- C. To provide medical assistance at accident scenes
- D. To asses the amount and scope of damage caused by the incident

Answer: D

NEW QUESTION 199

The process of applying secure configurations (to reduce the attack surface)

- A. Security Assessment
- B. Security Evaluation
- C. Security Benchmark
- D. Security Hardening

Answer: D

NEW QUESTION 202

What is the primary goal of implementing input validation in application security?

- A. To ensure all inputs are stored in a secure database
- B. To prevent unauthorized access to the application
- C. To validate and sanitize user inputs to prevent code injection attacks (Correct)
- D. To encrypt sensitive data transmitted between the client and server

Answer: C

NEW QUESTION 207

Which is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target

- A. MITRE ATT&CK
- B. CVE
- C. Risk Management framework
- D. Security Management

Answer: A

NEW QUESTION 211

Natalia is concerned about the security of his organization's domain name records and would like to adopt a technology that ensures their authenticity by adding digital signatures. Select the MOST appropriate technology to use?

- A. DNSSIGN
- B. DNSSEC
- C. CERTDNS
- D. DNS2

Answer: B

NEW QUESTION 212

A collection of actions that must be followed in order to complete a task or process in accordance with a set of rules

- A. Policy
- B. Procedure
- C. Law
- D. Standard

Answer: B

NEW QUESTION 216

What is the purpose of the CIA triad terms

- A. To make security more understandable to management and users
- B. To describe security using relevant and meaningful words
- C. To define the purpose of security
- D. All

Answer: D

NEW QUESTION 221

Why Red book is important in BCP

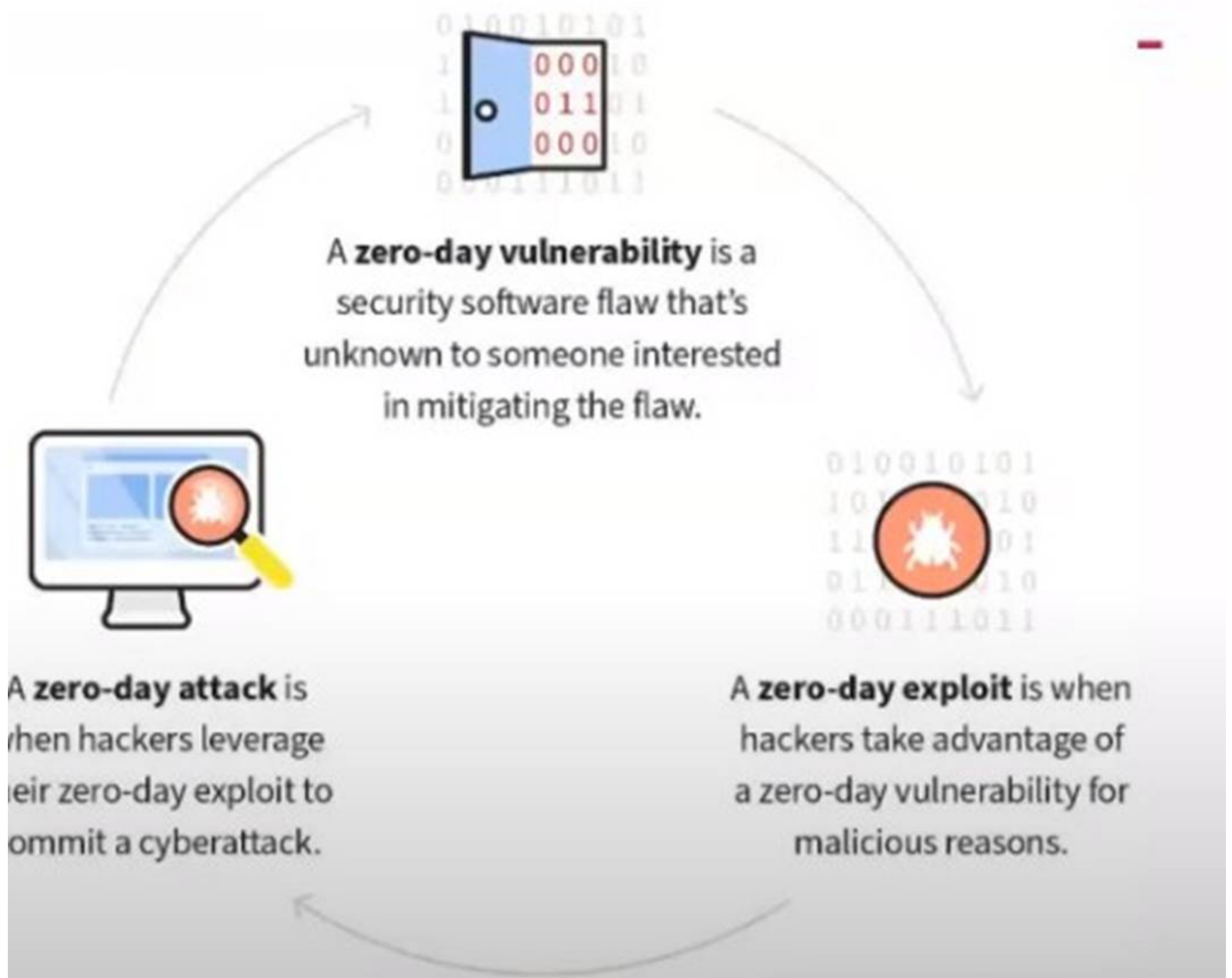
- A. To have hard copy for easy access
- B. Easy to carry and transfer
- C. A hurricane hits, the power is out and all the facilities are compromised and there is no access to electronic backups
- D. All

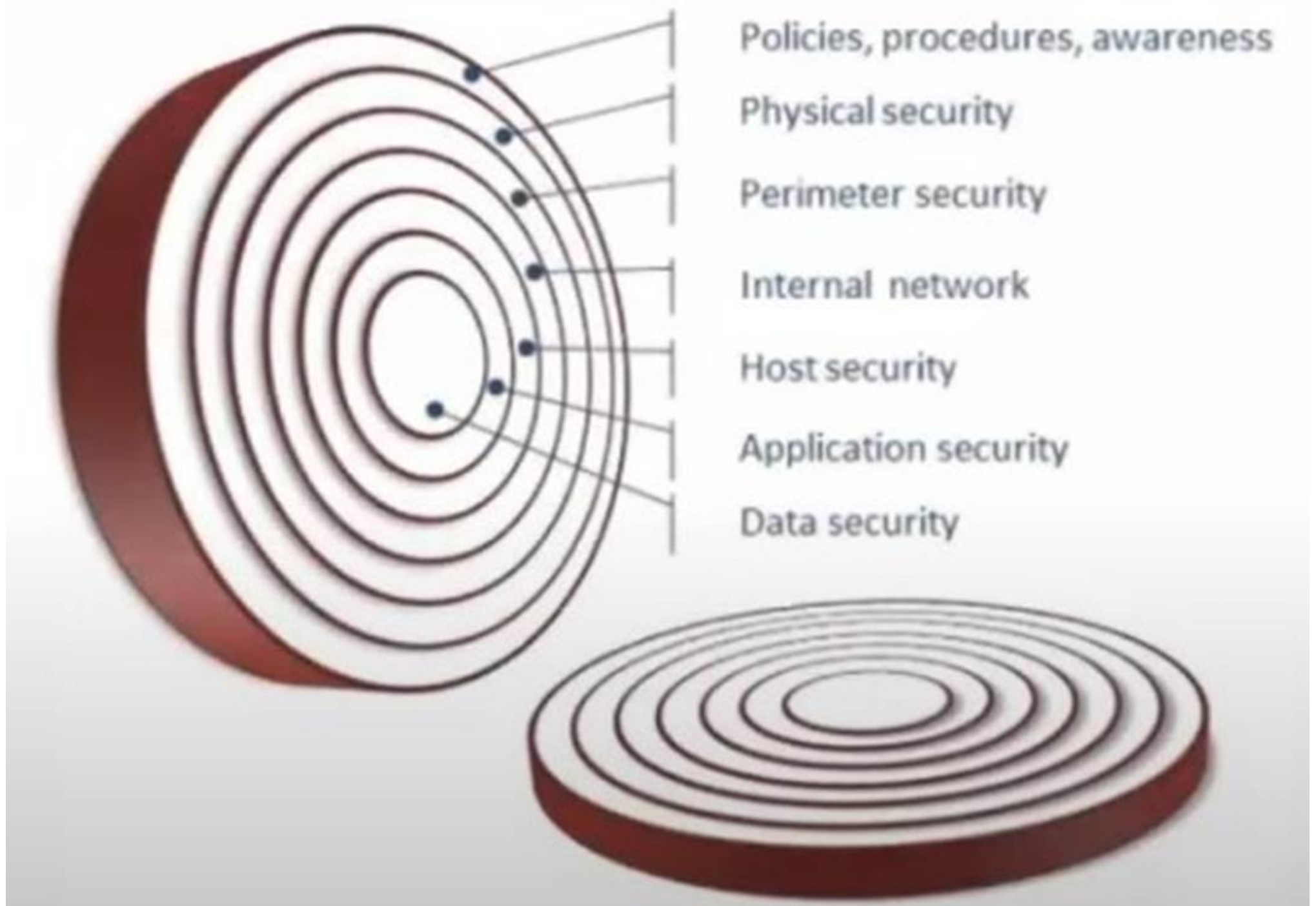
Answer: C

NEW QUESTION 223

Exhibit.

'Zero-Day' Defined





What kind of vulnerability is typically not identifiable through a standard vulnerability assessment?

- A. File permissions
- B. Buffer overflow
- C. Zero-day vulnerability
- D. Cross-site scripting

Answer: C

NEW QUESTION 225

Devid is worried about distributed denial of service attacks against his company's primary web application, which of the following options will provide the MOST resilience against large-scale ddos attacks?

- A. Implement a CDN
- B. Increase the number of servers in the web application server cluster
- C. Contract for DDoS mitigation services via the company's IPS
- D. Increase the amount of bandwidth available from one or more ISPs

Answer: A

NEW QUESTION 228

The prevention of authorized access to resources or the delaying of time critical operations.

- A. ARP Poisoning
- B. Syn Flood
- C. Denial-of-Service (DoS)
- D. All

Answer: C

NEW QUESTION 232

Port scanning attack target which OSI layer

- A. Layer 4
- B. Layer 3
- C. Layer 5
- D. Layer 6

Answer: A

NEW QUESTION 237

Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

- A. Breach
- B. Incident
- C. Adverse Event
- D. Exploit

Answer: C

NEW QUESTION 242

A Company critical functions were disrupted due to a system outage. What plan should the organization have in place to sustain these operations during and after a significant disruption?

- A. DRP
- B. BCP
- C. IRP
- D. ALL

Answer: B

NEW QUESTION 245

EKristol is the security administrator for a large online service provider. Kristal learns that the company is harvesting personal data of its customers and sharing the data with local governments where the company operates, without the knowledge of the users, to allow the governments to persecute users on the basis of their political and philosophical beliefs. The published user agreement states that the company will not share personal user data with any entities without the users' explicit permission. According to the ISC2 Code of Ethics, to whom does Kristal ultimately report in this situation?

- A. The company Kristal works for
- B. The governments of the countries where the company operates
- C. ISC2
- D. The users

Answer: D

NEW QUESTION 246

Which device is used to control traffic flow in network

- A. SDN
- B. Switch
- C. Hub
- D. Router

Answer: D

NEW QUESTION 251

.....

Relate Links

100% Pass Your CC Exam with Examible Prep Materials

<https://www.exambible.com/CC-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>