# 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**
What federal law requires the use of vulnerability scanning on information systems operated by federal government agencies?

A. FISMA
B. HIPAA
C. GLBA
D. FERPA

**Answer:** A

**NEW QUESTION 2**
What is the recommended fire suppression system for server rooms

A. Foam based
B. Water based
C. Powder based
D. ftac hacorl

**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**
Example of Dynamic authorization

A. DAC
B. RBAC
C. MAC
D. ABAC

**Answer:** D

**NEW QUESTION 5**
What is the importance of non-repudiation in todays world of ecommerce

A. It ensures that people are not held responsible for transaction that did not conduct
B. It ensures that people are held responsible for transactions they conducted
C. It ensures that transactions are not conducted online
D. It ensures that transactions are conducted online

**Answer:** B

**NEW QUESTION 6**
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. Administratirve Access control

**Answer:** A

**NEW QUESTION 7**
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 8**
Part of a zero-trust strategy that breaks LANs into very small and highly localized zones using firewalls.

A. Zero Trust
B. DMZ
C. VPN
D. Micro Segmentation

**Answer:** D

**NEW QUESTION 9**
In Which of the following access control models can the creator of an object delegate permission

A. MAC
B. RBAC
C. ABAC
D. DAC

**Answer:** C

**NEW QUESTION 10**
255.255.255.0 Address represents

A. Broadcast
B. Unicast
C. Subnet mask
D. Global Address

**Answer:** C

**NEW QUESTION 10**
What is the first phase in System Development Life Cycle

A. Requirements Analysis Phase
B. Feasibilty Study
C. Design Phase
D. Development Phase

**Answer:** B

**NEW QUESTION 15**
Which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

A. VLAN
B. SDN
C. VPN
D. SAN

**Answer:** B

**NEW QUESTION 20**
Which of the following is not a Social engineering technique

A. Pretexting
B. Baiting
C. Quid pro quo
D. Double Dealing

**Answer:** D

**NEW QUESTION 25**
A organization's security system which involves in preventing, detecting, analyzing, and responding to cybersecurity incidents.

A. Business continuity team
B. Disaster recovery team
C. Incident response team
D. Security operations center

**Answer:** D

**NEW QUESTION 30**
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 31**
Which OSI layer VPN works

A. Layer 5
B. Layer 6
C. Layer 1
D. Layer 3

**Answer:** D

**NEW QUESTION 33**
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 36**
A popular way of implementing "least privilege"

A. MAC
B. DAC
C. RBAC
D. ABAC

**Answer:** C

**NEW QUESTION 37**
Which type of control is used to minimize the impact of an attack and to restore normal operations as quick as possible

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

**Answer:** C

**NEW QUESTION 41**
What is meant by non-repudiation?

A. If a user does something, they can't later claim that they didn't do it.
B. Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.
C. It is part of the rules set by administrative controls.
D. It is a security feature that prevents session replay attacks.

**Answer:** A

**NEW QUESTION 46**
Also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs)

A. Hypervisor
B. Simulation
C. Emulation
D. Cloud Controller

**Answer:** A

**NEW QUESTION 49**
Embedded systems and network-enabled devices that communicate with the internet are considered as

A. Endpoint
B. Node
C. IOT
D. Router

**Answer:** C

**NEW QUESTION 54**

DNS works in which OSI layer

A. Physical Layer
B. Network Layer
C. Application layer
D. DataLink Layer

**Answer:** C

**NEW QUESTION 56**
Timiting access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity.

A. DAC
B. MAC
C. RuBAC
D. RBAC

**Answer:** B

**NEW QUESTION 58**
Which element of the security policy framework includes recommendation that are NOT bindings?

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

**Answer:** C

**NEW QUESTION 63**
The common term used to describe the mechanisms that control the temperature and humidity in a data center

A. VLAN (virtual local area network)
B. STAT (system temperature and timing)
C. TAWC (temperature and water control)
D. HVAC (heating, ventilation and air conditioning)

**Answer:** D

**NEW QUESTION 65**
What is a type of system architecture where a single instance can serve multiple distinct user groups.

A. Mutli-threading
B. Multi-processing
C. Multitenancy
D. Multi-cloud

**Answer:** C

**NEW QUESTION 68**
What is the range of well known ports

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

**Answer:** A

**NEW QUESTION 73**
The documentation of a predetermined set of instructions or procedures to detect, respond to andlimit consequences of a malicious cyberattack against an organization's information systems(s).

A. IR
B. IRP
C. BCP
D. DRP

**Answer:** B

**NEW QUESTION 75**
Port forwarding is also known as

A. Port mapping

B. Tunneling
C. Punch through
D. ALL

**Answer:** D

**NEW QUESTION 77**
Which of the following is endpint

A. Router
B. Firewall
C. Laptop
D. Switch

**Answer:** C

**NEW QUESTION 80**
Which layer does VLAN hopping belong to?

A. Layer 3
B. Layer 4
C. Layer 7
D. Layer 2

**Answer:** D

**NEW QUESTION 85**
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 86**
What is the best practise to clear SSD storage after usage in term of cyber security

A. Zero fill
B. Degaussing
C. Clearing
D. Disintegration

**Answer:** D

**NEW QUESTION 87**
In information systems terms, the activities necessary to restore IT and communications services of an organization during and after an outage

A. IR
B. BC
C. Risk Management
D. DR

**Answer:** D

**NEW QUESTION 91**
What security feature used in HTTPS

A. IPSec
B. SSH
C. ICMP
D. SSL/TLS

**Answer:** D

**NEW QUESTION 95**
A cyber security professional observes an unusual occurrence in the network or system. What term best describes this situations

A. Breach
B. Exploit
C. Event
D. Intrusion

**Answer:** C

**NEW QUESTION 97**
Difference between Sniffing and Snooping

A. Sniffing is the process of intercepting and collecting network traffic as it passes over a digital networ
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 networ
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 snoofing is a thread

**Answer:** A

**NEW QUESTION 101**
Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Micro segmentation of workloads is a tool of the model

A. Zero Trust
B. Defence in Depth
C. Least Privileges
D. AII

**Answer:** A

**NEW QUESTION 104**
While taking the certification exam for ISC2 CC, You notice another candidate for the certification cheating. What should you do?

A. Yell at the other candidate for violating test security.
B. Nothing—each person is responsible for their own actions.
C. Report the candidate to ISC2.
D. Call local law enforcement.

**Answer:** C

**NEW QUESTION 108**
Is an integrated platform and graphical tool for performing security testing of web applications.

A. Burb suite
B. Wireshark C Fiddler
C. ZenMap

**Answer:** A

**NEW QUESTION 109**
Which of the following attacks can TLS help mitigate?

A. Cross-site Scripting (XSS) Attacks
B. Social Engineering Attacks
C. Man-in-the-middle (MiTm) Attacks (Correct)
D. SQL Injection Attacks

**Answer:** C

**NEW QUESTION 110**
Which threats are directly associated with malware? Select that apply.

A. APT
B. Ransomeware
C. Trojan
D. DDOS

**Answer:** C

**NEW QUESTION 113**
What is the primary goal of network segmentation in cybersecurity?

A. To increase network speed
B. To isolate and protect critical assets
C. To centralize data storage
D. To expand the network's coverage

**Answer:** B

**NEW QUESTION 114**
In DAC, the policy specifies that a subject who has been granted access to information can do the following:

A. Change security attributes on subjects, objects, information systems or system components
B. Choose the security attributes to be associated with newly created or revised objects
C. Change the rules governing access control
D. ALL

**Answer:** D

**NEW QUESTION 119**
Which of the following is NOT one of the four typical ways of managing risk?

A. Accept
B. Avoid
C. Mitigate
D. Monitor

**Answer:** D

**NEW QUESTION 122**
Which is an authorized simulated attack performed on a computer system to evaluate its security.

A. Penetration test
B. Security Testing
C. Automated Testing
D. Regression Testing

**Answer:** A

**NEW QUESTION 123**
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 128**
What is the primary purpose of a firewall in network security?

A. Encrypt data transmissions
B. Prevent unauthorized access
C. Monitor network traffic
D. Backup critical data

**Answer:** B

**NEW QUESTION 129**
Which of the following is a characteristic of cloud

A. Broad Network Access
B. Rapid Elasticity
C. Measured Service
D. AII

**Answer:** B

**NEW QUESTION 132**
Which type of software testing focuses on examining the source code for vulnerabilities and security issues?

A. Black-box testing
B. White-box testing
C. Functional testing
D. User acceptance testing

**Answer:** B

**NEW QUESTION 134**
Which of the following is not a source of redundant power

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

**Answer:** D

**NEW QUESTION 137**
Which of these tool is commonly used to crack passwords

A. Bup Suite
B. Nslookup
C. Wireshark
D. John the ripper

**Answer:** D

**NEW QUESTION 138**
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 142**
Created by switches to logically segment a network without altering its physical topology.

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

**Answer:** C

**NEW QUESTION 143**
Exhibit.


information security is not built on which of the following?

A. Confidentiality
B. Availability
C. Accessibility
D. Integrity

**Answer:** C

**NEW QUESTION 147**
Which addresses reserved for internal network use and are not routable on the internet.

A. acOO:: to adff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
B. fcOO:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
C. bcOO:: to bdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
D. ccOO:: to cdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

**Answer:** B

**NEW QUESTION 149**
Communication between end systems is encrypted using a key, often known as _____?

A. Temporary Key
B. Section Key
C. Public Key
D. Session Key

**Answer:** D

**NEW QUESTION 150**

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 155**
If a device is found that is not compliant with the security baseline, what will be the security team action

A. Report
B. Evaluate
C. Ignore
D. Disabled or isolated into a quarantine area until it can be checked and updated.

**Answer:** D

**NEW QUESTION 157**
A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time.

A. Spoofing
B. Phishing
C. DOS
D. Advanced Persistent Threat

**Answer:** D

**NEW QUESTION 160**
Which maintains that a user or entity should only have access to the spec data, resources and applications needed to complete a required task.

A. Zero Trust
B. Defence in Depth
C. Least Privileges
D. AII

**Answer:** C

**NEW QUESTION 165**
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 167**
Organization experiences a security event that does not affect the confidentiality integrity and availability of its information system. What term BEST describes this situation?

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

**Answer:** D

**NEW QUESTION 169**
A type of malware that is capable of self propagation and can infect multiple systems on network without the need for human intervention

A. Worm
B. Spy ware
C. Adwre
D. Virus

**Answer:** A

**NEW QUESTION 174**
A company performs an analysis of its information systems requirements functions and interdependences in order to prioritize contingency requirement. What is this process called?

A. BCP

B. DRP
C. IRP
D. BIA

**Answer:** D

**NEW QUESTION 179**
A company has implemented Mandatory access control for its confidential data which of the following statement is true

A. The data can be accessed by users who possess a need to know
B. Access controls cannot be changed by anyone except the system administrato
C. The owner of the data can modify the access control
D. The system adminstrator can change the access contrls

**Answer:** B

**NEW QUESTION 181**
Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?

A. Routers
B. Laptops
C. Firewalls
D. Backups

**Answer:** D

**NEW QUESTION 186**
What is the priority of incident response in the context of incident management

A. Protect the organization mission and objectives
B. Reduce the impact of the incident
C. Protect life health and safety
D. Resume interrupted operations as soon as possible

**Answer:** C

**NEW QUESTION 188**
Mark is configuring an automated data transfer between two hosts and is choosing an authentication technique for one host to connect to the other host. What approach would be best-suited for this scenario?

A. Biometric
B. Smart Card
C. SSH Key
D. Hard Coded Password

**Answer:** C

**NEW QUESTION 191**
Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

A. Segment
B. Packet
C. Frame
D. None of the Above

**Answer:** B

**NEW QUESTION 192**
John was recently offered a consulting opportunity as a side job. He is concerned that this might constitute a conflict of interest. Which one of the following sources that he needs to refer to take an appropriate decision?

A. ISC2 Code of ethics
B. Organizational code of ethics
C. Country code of ethics
D. Organizational security policy

**Answer:** B

**NEW QUESTION 195**
What is the benefit of subnet

A. By increasing network bandwidth
B. By improving network security
C. By reducing network congestion
D. By simplifying network management

**Answer:** C

**NEW QUESTION 197**
The Bell and LaPadula access control model is a form of

A. RBAC
B. MAC
C. DAC
D. ABAC

**Answer:** B

**NEW QUESTION 199**
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information

A. Risk Management
B. Risk Assessment
C. Risk Mitigation
D. Adequate Security

**Answer:** D

**NEW QUESTION 200**
Which type of application can intercept sensitive information such as passwords on a network segment?

A. Log server
B. Network Scanner
C. Firewall
D. Protocol Analyzer

**Answer:** D

**NEW QUESTION 201**
Example of Deterrent controls

A. CCTV
B. BCP
C. DRP
D. IRP

**Answer:** A

**NEW QUESTION 203**
Which type of authentication is something which you

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

**Answer:** C

**NEW QUESTION 204**
Natalia is concerned that users on her network may be storing sensitive information, such as social security numbers, on their hard drives without proper authorization or security controls. What 3rd -party security service can she implement to best detect this activity?

A. IDS - Intrusion Detection System
B. IPS - Intrusion Prevention System
C. DLP - Data Loss Protection
D. TLS - Transport Layer Security

**Answer:** C

**NEW QUESTION 209**
What is the process of verifying a users identity called?

A. Confidentiality
B. Autentication
C. Authorization
D. Identification

**Answer:** B

**NEW QUESTION 211**

Which document serve as specifications for the implementation of policy and dictates mandatory requirements

A. Policy
B. Guideline
C. Standard
D. Procedures

**Answer:** C

**NEW QUESTION 212**
Which security control mostly used to prevent data breach

A. Physical control
B. Logical Control
C. Adminstrative Control
D. RBAC

**Answer:** B

**NEW QUESTION 214**
Why is security training important?

A. Because it fulfills regulatory requirements.
B. Because it helps people to perform their job duties more efficiently.
C. Because it reduces the risk of certain types of attacks, like social engineering.
D. AII

**Answer:** C

**NEW QUESTION 219**
Exhibit.

| Symmetric Encryption | Asymmetric Encryption |
| --- | --- |
| • Symmetric encryption consists of one key for encryption and decryption. | • Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**. |
| • Symmetric Encryption is a lot quicker compared to the Asymmetric method. | • As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably. |
| • RC4<br>• AES<br>• DES<br>• 3DES<br>• QUAD | • RSA<br>• Diffie-Hellman<br>• ECC<br>• El Gamal<br>• DSA |

How many keys would be required to support 50 users in an asymmetric cryptography system?

A. 100
B. 200
C. 50
D. 1225

**Answer:** A

**NEW QUESTION 222**
Restoring IT and communications back to full operation after a disruption.

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

**Answer:** C

**NEW QUESTION 227**
Which of these is an example of deterrent control

A. Biometric
B. Guard Dog
C. Encryption
D. Trunstile

**Answer:** B

**NEW QUESTION 228**
Which is strongly used for Securing Wi-Fi

A. WPA2
B. WEP
C. WPA
D. SSL

**Answer:** A

**NEW QUESTION 232**
Measure of the extent to which an entity is threatened by a potential circumstance or event and likelihood of occurrence

A. Impact
B. Risk
C. Threat
D. Threat Vector

**Answer:** B

**NEW QUESTION 233**
Devid's team recently implemented a new system that gathers information from a variety of different log sources, analyses that information, and then triggers automated playbooks in response to security events, what term BEST describes this technology?

A. SIEM
B. Log Repository
C. IPS
D. SOAR

**Answer:** D

**NEW QUESTION 235**
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 237**
An employee unintentionally shares confidential information with an unauthorized party. What term best describes this situation?

A. Event
B. Exploit
C. Intrusion
D. Breach

**Answer:** D

**NEW QUESTION 242**
Granting a user access to services or the system

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

**Answer:** C

**NEW QUESTION 245**
WF attack in which a subscriber currently authenticated to an Server and connected through a secure session browses to an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the Server

A. XSS
B. CSRF
C. Spoofing
D. ALL

**Answer:** B

**NEW QUESTION 247**
The purpose of risk identification:

A. Employees at all levels of the organization are responsible for identifying risk.
B. Identify risk to communicate it clearly.
C. Identify risk to protect against it.
D. ALL

**Answer:** D

**NEW QUESTION 248**
When the ISC2 Mail server sends mail to other mail servers it becomes —?

A. SMTP Server
B. SMTP Peer
C. SMTP Master
D. SMTP Client

**Answer:** D

**NEW QUESTION 250**
Which type of attack attempts to gain information by observing the devices power consumption

A. DOS
B. Side Channles
C. XSS
D. XSRF

**Answer:** B

**NEW QUESTION 252**
What is the purpose of multi-factor authentication (MFA) in 1AM?

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 257**
What is the purpose of immediate response procedures and checklists in a BCP

A. To notify personnel that the BCP is being enacted
B. To provide guidance for management
C. To safeguard the confidentiality, integrity and availability of information
D. To ensure business operations are accounted for in the plan

**Answer:** A

**NEW QUESTION 261**
What cybersecurity principle focuses on granting users only the privileges necessary to perform their job functions?

A. Least privilege (Correct)
B. defense in depth
C. separation of duties
D. need-to-know basis

**Answer:** A

**NEW QUESTION 263**
Permitting authorized access to information while protecting it from improper disclosure

A. Integrity
B. Confidentiality
C. Availability
D. ALL

**Answer:** B

**NEW QUESTION 264**
Example of Type 1 Authentication

A. Password
B. Smart Card
C. Finger Print
D. RSA Token

**Answer:** A

**NEW QUESTION 266**
Which access control model can grant access to a given object based on complex rules

A. ABAC
B. DAC
C. MAC
D. RBAC

**Answer:** A

**NEW QUESTION 270**
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 272**
What is Remanence

A. The ability of retaining magnetization in storage disk after deletion
B. Files or pieces of files get scattered throughout your disks.
C. Data corruption due to disk failure
D. AII

**Answer:** A

**NEW QUESTION 274**
Which one of the following cryptographic algorithms does not depend upon the prime factorization problem?

A. RSA - Rivest-Shamir-Adleman
B. GPG - GNU Privacy Guard
C. ECC - Elliptic curve cryptosystem
D. PGP - Pretty Good Privacy

**Answer:** C

**NEW QUESTION 279**
Which of the following physical controls is used to protect against eavesdropping and data theft through electromagnetic radiation

A. EMI Shielding
B. Screening rooms
C. White noise generators
D. ALL

**Answer:** A

**NEW QUESTION 280**
What is the primary goal of the incident management team in the organization

A. Reduce the impact and resore services
B. Gathering and analyzing information
C. Conducting Leason learn meeting
D. RCA of the impact

**Answer:** A

**NEW QUESTION 285**

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 288**
Which type of network is set up similar to the internet but is private to an organization. Select the MOST appropriate?

A. Extranet
B. VLAN
C. Intranet
D. VPN

**Answer:** B

**NEW QUESTION 291**
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 294**
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 299**
An outward-facing IP address used to access the Internet.

A. Global Address
B. Private Address
C. Public Address
D. DNS

**Answer:** C

**NEW QUESTION 301**
Which protocol is used for secure email

A. POP3S
B. IMAPS
C. SMTPS
D. AII

**Answer:** D

**NEW QUESTION 303**
What does the term "Two-factor authentication" refer to in Cybersecurity?

A. Using two different antivirus programs
B. Verifying identity with two independent factors
C. Accessing two different networks simultaneously
D. Changing passwords every two weeks

**Answer:** B

**NEW QUESTION 304**
Which of the following does not normally influence an organization's retention policy for logs?

A. Laws
B. Corporate governance
C. Regulations

D. Audits

**Answer:** D

**NEW QUESTION 306**
What is the primary purpose of a honeytoken in cybersecurity?

A. To lure and detect attackers
B. To encrypt sensitive data
C. To enhance network performance
D. To manage user access

**Answer:** A

**NEW QUESTION 309**
An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

A. BIA
B. DR
C. BCP
D. IRP

**Answer:** A

**NEW QUESTION 313**
A common network device used to filter traffic?

A. Server
B. Endpoint
C. Ethernet
D. Firewa

**Answer:** D

**NEW QUESTION 315**
The primary goal of a risk assessment

A. Avoid Risk
B. Estimate and Prioritize Risk
C. Ignore risk
D. Evaluate the Impact

**Answer:** B

**NEW QUESTION 317**
Set of rules that everyone must comply with and usually carry monetary penalties for noncompliance

A. Standard
B. Policy
C. Procedure
D. Laws or Regulations

**Answer:** A

**NEW QUESTION 318**
Government can imposes financial penalties as a consequence of breaking a

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

**Answer:** B

**NEW QUESTION 319**
Which is not the function of IPS

A. To encrypt network traffic
B. To monitor network traffic
C. To filter network traffic
D. To detect and prevent attacks

**Answer:** A

**NEW QUESTION 322**
Which of the following properties is not guaranteed by Digital signatures

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

**Answer:** B

**NEW QUESTION 324**
A company's governing board may agree that legal services will examine any third-party contracts, so they create a _____ stating that aside from legal services, no other department in the companvhahppn pivpn nprmkcinn to review third-party contracts

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

**Answer:** B

**NEW QUESTION 325**
What is the purpose of the CIA triad terms

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

**Answer:** D

**NEW QUESTION 329**
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. AII

**Answer:** C

**NEW QUESTION 334**
What is the most important aspect of security awareness/training?

A. Maximizing business capabilities
B. Protecting assets
C. Protecting health and human safety
D. Ensuring the confidentiality of data

**Answer:** C

**NEW QUESTION 339**
A company primary data center goes down due to a hardware failure causing a major disruption to the IT and communications systems. What is the focus of disaster recovery planning in this scenario

A. Maintaining critical business functions during the disruption
B. Fixing the hardware failure
C. Restoring IT and communication system back to full operations after the disruptions.
D. Guiding the actions of emergency response personnel during the disruption

**Answer:** C

**NEW QUESTION 341**
Protection against an individual falsely denying having performed a particular action

A. Authentication
B. Identification
C. Verification
D. Non repudiation

**Answer:** D

**NEW QUESTION 344**
What is the BEST defense against dumpster diving attacks?

A. Anti-malware software
B. Clean desk policy
C. Data loss prevention tools
D. Shredding

**Answer:** D

**NEW QUESTION 349**
An attackers place themselves between two devices (often a web browser and a web server)

A. Phishing
B. Spoofing
C. On Path
D. All

**Answer:** C

**NEW QUESTION 350**
DDOS attack affect which OSI layer

A. Network layer
B. Transport layer
C. Physical Layer
D. Both A and B

**Answer:** D

**NEW QUESTION 353**
Which of these is the most efficient and effective way to test a business continuity plan

A. Simulations
B. Discussions
C. Walkthroughs
D. Reviews

**Answer:** A

**NEW QUESTION 354**
What does the term business in business continuity planning refer to?

A. The financial performance of the organization
B. The technical systems of the organization
C. The operation aspects of the organization
D. The physical infrastructure of the organization

**Answer:** C

**NEW QUESTION 356**
Port scanning attack target which OSI layer

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

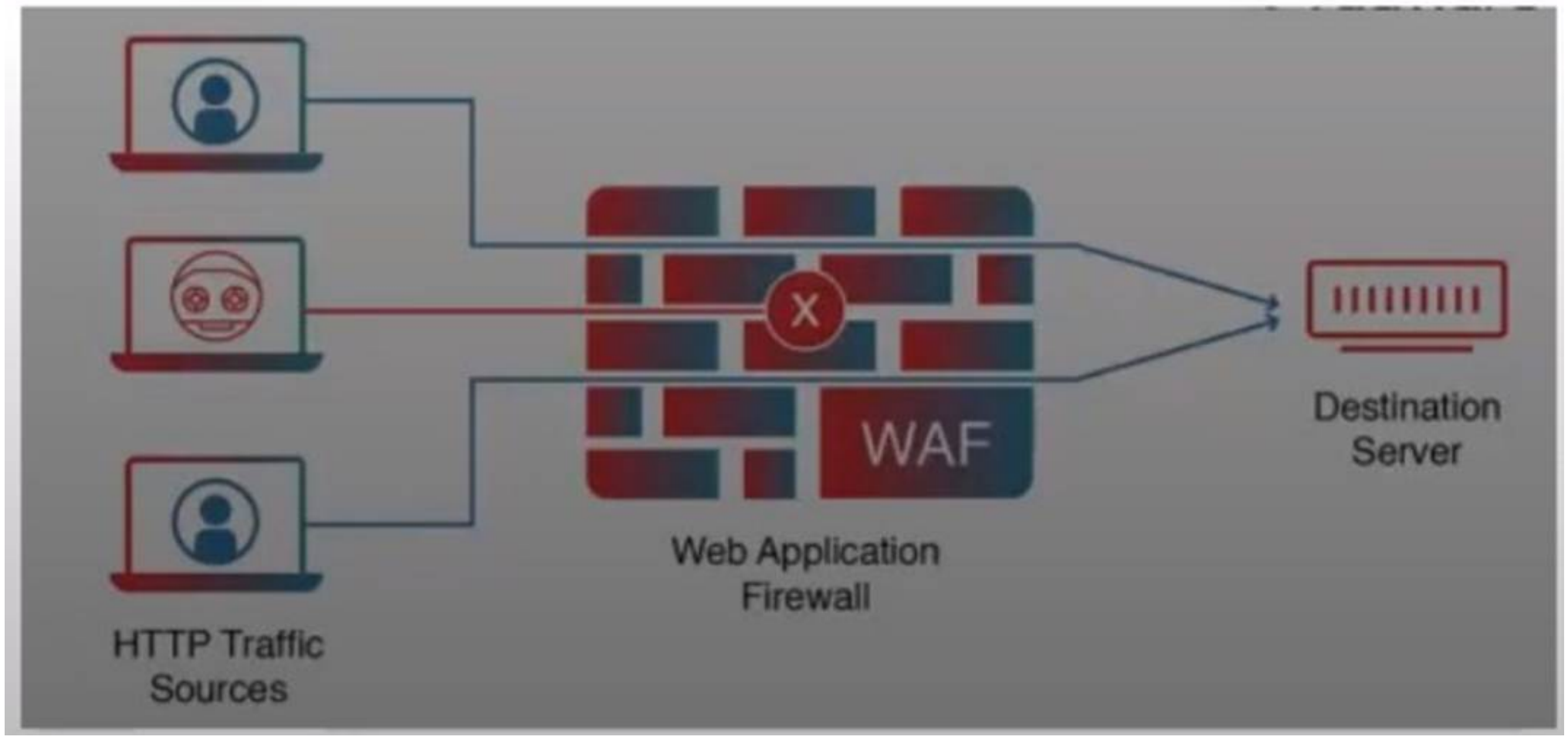
**Answer:** A

**NEW QUESTION 361**
Which is not possible models for an Incident Response Team (IRT):

A. Leveraged
B. Dedicated
C. Hybrid
D. Outsourced

**Answer:** D

**NEW QUESTION 362**
Exhibit.




What is the PRIMARY purpose of a web application firewall (WAF)?

A. To protect the web server from DDoS attacks
B. To monitor network traffic for intrusions
C. To filter and block malicious web traffic and requests
D. To manage SSL certificates

**Answer:** C

**NEW QUESTION 365**
A hacker is trying to gain access to a company network which of the following scenarios would be an example of defense in depth

A. The company relies solely on a firewall to block unauthorized access
B. The company stores all sensitive data on a single server
C. The hacker is required to enter a username and password
D. None

**Answer:** C

**NEW QUESTION 366**
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 368**
The harmonization of automated computing tasks, providing a consolidated and reusable workflow

A. Cloud Orchestration
B. Cloud Manager
C. Cloud broker
D. Cloud Controller

**Answer:** A

**NEW QUESTION 372**
A Company critical functions were disrupted due to a system outage. What plan should theorganization have in place to sustain these operations during and after a significant disruptions?

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

**Answer:** B

**NEW QUESTION 376**
Token Ring used in which OSI Layer

A. Application
B. Network
C. Transport
D. Physical

**Answer:** D

**NEW QUESTION 381**
Methods or mechanisms cybercriminals use to gain illegal, unauthorized access to computer systems and networks.

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

**Answer:** B

**NEW QUESTION 385**
.....

# Relate Links

**100% Pass Your CC Exam with Exambible 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/