# Exam Questions CC

Certified in Cybersecurity (CC)

**https://www.2passeasy.com/dumps/CC/**

**NEW QUESTION 1**
How do you distinguish Authentication and Identification

A. Both Same
B. Authentication is the process of verifying user identity and a user of a system or an application
C. Authentication is the process of verifying user identity and Identification is the ability to identify uniquely quely Identification is the process to allow resource access
D. Identification is the process of verifying user identity and Authentication is the process to allow resource access

**Answer:** B

**NEW QUESTION 2**
Example of Dynamic authorization

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

**Answer:** D

**NEW QUESTION 3**
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 4**
255.255.255.0 Address represents

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

**Answer:** C

**NEW QUESTION 5**
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 6**
Example of Token based Authentication

A. Kerberos
B. Basic
C. OAuth
D. NTLN

**Answer:** C

**NEW QUESTION 7**
TCP and UDP reside at which layer of the osi model?

A. Session
B. Transport
C. Data link
D. Presentation

**Answer:** D

**NEW QUESTION 8**

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 9**
Mark has purchased a MAC LAPTOP. He is scared of losing his screen and planning to buy an insurance policy. So, which risk management strategy is?

A. Risk acceptance
B. Risk deterrence
C. Risk transference
D. Risk mitigation

**Answer:** C

**NEW QUESTION 10**
Which of the following is not a protocol of the OSI layer 3

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

**Answer:** D

**NEW QUESTION 10**
What is the primary goal of incident management

A. To potect life health and safety
B. To reduce the impacrt of an incident
C. To prepare for any incident
D. To resume interrupted operations as soon as possible

**Answer:** C

**NEW QUESTION 14**
What type of attack does the attacker store and reuse login information. Select the BEST answer?

A. Man-in-the-middle attack
B. Smurf attack
C. DDoS attack
D. Replay attack

**Answer:** D

**NEW QUESTION 17**
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 19**
Which drives for the IPv6 introduction

A. IPv4 was not secured
B. IPv4 not combatible with new devices
C. Because IPv4 was projected to be exhausted
D. IPV6 support WiFi

**Answer:** C

**NEW QUESTION 22**
What is the importance of identifying roles and responsibilities in incident response planning?

A. To prevent incidents from happening
B. To ensure that everyone knows their job in the incident response process

C. To reduce the impact of the incident
D. To choose an appropriate containment strategy

**Answer:** B

**NEW QUESTION 25**
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 29**
Which type of attack takes advantage of vulnerabilities in validation?

A. ARP spoofing
B. Pharming attacks
C. Cross-site scripting (XSS)
D. DNS poisoning

**Answer:** C

**NEW QUESTION 34**
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 39**
What is the main purpose of using multi-factor authentication (MFA) in a security system?

A. To prevent data breaches
B. To protect against malware
C. To ensure data integrity
D. To add an extra layer of security to user authentication

**Answer:** D

**NEW QUESTION 41**
Scans networks to determine everything that is connected as well as other information.

A. Burbsuite
B. Wireshark
C. Fiddler
D. Zen Mao

**Answer:** D

**NEW QUESTION 46**
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 47**
Are a measure of an organization's baseline of security performance

A. Security Assessment
B. Secuirty Audit
C. Security Benchmark
D. Security Management

**Answer:** C

**NEW QUESTION 50**
Which TLS extension is used to optimize the TLS handshake process by reducing the number of round trips between the client and server?

A. TLS Renegotiation
B. TLS Heartbeat
C. TLS Session Resumption
D. TLS FastTrack

**Answer:** C

**NEW QUESTION 55**
Which of the following is a subject?

A. file
B. fence
C. filename
D. user

**Answer:** D

**NEW QUESTION 56**
Which layer does VLAN hopping belong to?

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

**Answer:** D

**NEW QUESTION 60**
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 61**
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. Authetication
C. Authentication
D. Availablity

**Answer:** A

**NEW QUESTION 66**
which is the short form of IPv6 address 2001:0db8:0000:0000:0000:ffff:0000:0001

A. 2001:db8::ffff:0:1
B. 2001:db8:0000:ffff:0:1
C. 2001:db80::ffff:0000:1
D. 2001:db8::ffff:0000:0001

**Answer:** A

**NEW QUESTION 70**
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 75**
Information should be consistently and readily accessible for authorized parties ?

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

**Answer:** C

**NEW QUESTION 76**
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 80**
Which Prevents Threat

A. Antivirus
B. IDS
C. SIEM
D. HIDS

**Answer:** A

**NEW QUESTION 85**
A security practitioner who needs step-by-step instructions to complete a provisioning task

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

**Answer:** C

**NEW QUESTION 89**
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 94**
In what way do a victim's files get affected by ransomware?

A. By destroying them
B. By encrypting them
C. By stealing them
D. By selling them

**Answer:** B

**NEW QUESTION 98**
Which threats are directly associated with malware? Select that apply.

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

**Answer:** C

**NEW QUESTION 101**
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 105**
A structured approach used to oversee and manage risk for an enterprise

A. Risk Assessment
B. Risk threshold
C. Risk Management Framework
D. Risk appetite

**Answer:** C

**NEW QUESTION 106**
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 111**
Which of the following uses registered port

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

**Answer:** D

**NEW QUESTION 115**
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 119**
Which is the loopback address

A. ::1
B. 127.0.0.1
C. 255.255.255.0
D. Both A and B

**Answer:** D

**NEW QUESTION 123**
The means by which a threat actor carries out their objectives

A. Threat
B. Threat Vector
C. Exploit
D. Intrusion

**Answer:** B

**NEW QUESTION 125**
How many bits represent the organization unique identifier (oui) in mac addresses?

A. 16 Bits
B. 48 Bits
C. 24 Bits
D. 32 Bits

**Answer:** C

**NEW QUESTION 126**
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 130**
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 132**
Some Employee of his organization launched a privilege escalation attack to gain root access on one of the organization's database serversiThe employee does have an authorized user account on the server. What log file would be MOST likely to contain relevant information??

A. Database application log
B. Firewall log
C. Operating system log
D. IDS log

**Answer:** C

**NEW QUESTION 135**
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 139**
Type of cyber attack carried out over a LAN that involves sending malicious packets to a default gateway on a LAN

A. ARP Poisoning
B. Syn Flood
C. Ping of death
D. Trojan

**Answer:** A

**NEW QUESTION 142**
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 144**
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 147**
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 152**
What is IPSEC reply attack

A. An attack where an attacker modifies packets in transit
B. An attack where an attacker eavesdrops on network traffic
C. An attack where an attacker overloads a network with traffic
D. An attack where an attacker attempts to inject packets in an existing sessio

**Answer:** D

**NEW QUESTION 156**
When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called _____

A. Malware
B. Zero-day
C. Event
D. Attack

**Answer:** B

**NEW QUESTION 161**
The process of running a simulated instances of a computer system in a layer abstracted from the underlying hardware server or workstation

A. Containerization
B. Simulation
C. Emulation
D. Virtualization

**Answer:** D

**NEW QUESTION 163**
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

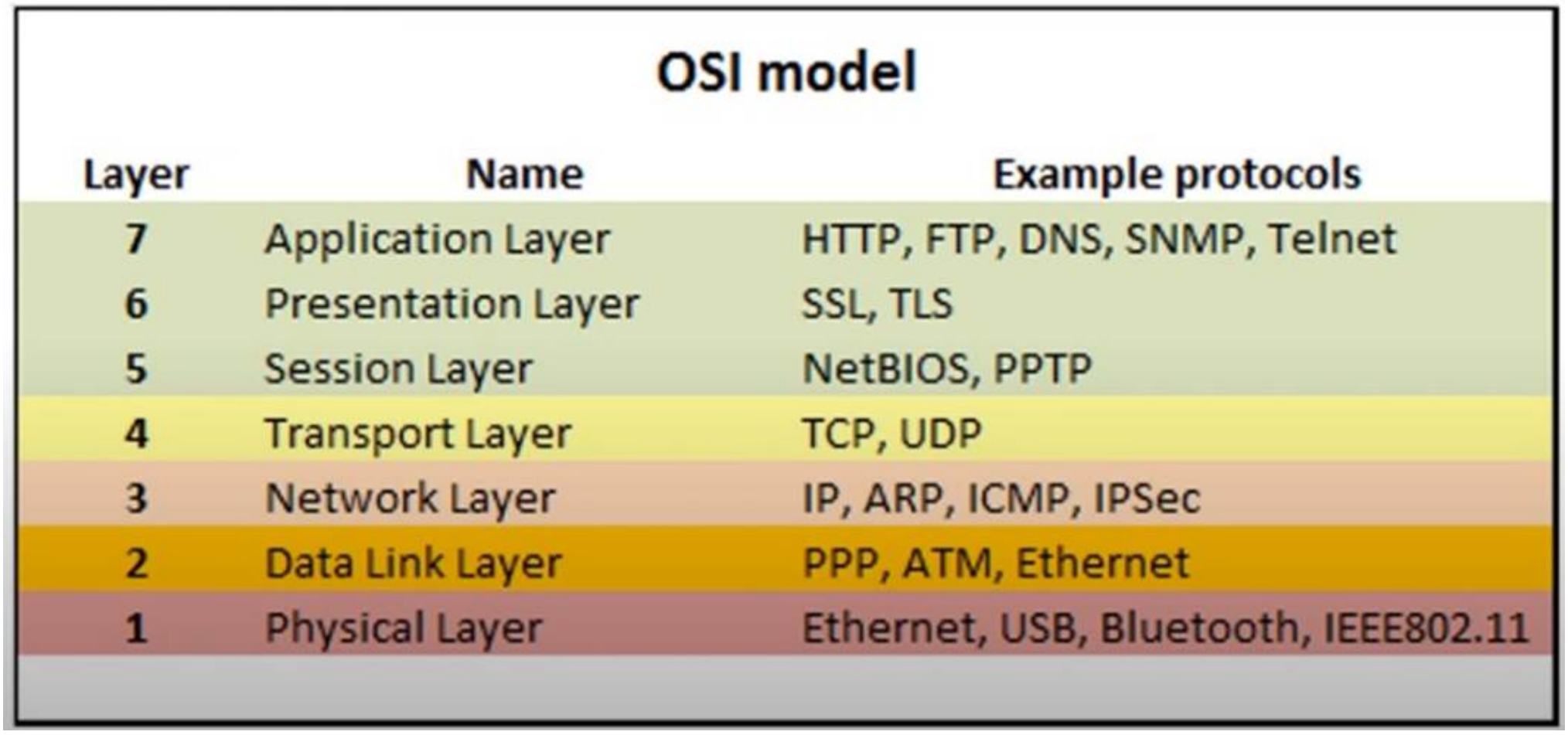
**Answer:** A

**NEW QUESTION 168**
Selvaa presents a userid and a password to a system in order to log on. Which of the following characteristics must the userid have?

A. Autherization
B. Authentication
C. Availability
D. Identification

**Answer:** D

**NEW QUESTION 169**
Exhibit.




IPSec works in which layer of OSI Model

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

**Answer:** C

**NEW QUESTION 172**
Which of the following best describes the puposes of a business impact analysis?

A. To document a predetermined set of instructions or procedures for restoring IT and communications services after a disruption
B. To mitigate security violation and ensure that business operation can continue during a contigency
C. To provide a high level overview of the disaster recovery plan
D. To analyze an information systems requirements and functions in order to determine system contingency priorities

**Answer:** D

**NEW QUESTION 175**
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 180**
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 182**
Which access control model is best suited for a large organization with many departments
that have different data access needs

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

**Answer:** B

**NEW QUESTION 187**
are events that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed

A. Exploit
B. Security Incident
C. Threat
D. Rreach

**Answer:** B

**NEW QUESTION 189**
Which type of attack will most effectively maintain remote access and control over the victims computer

A. Phising
B. Trojans
C. XSS
D. RootKits

**Answer:** D

**NEW QUESTION 193**
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 196**
What does internal consistency of information refer to

A. Data being accurate, usefull and complete
B. Data being protected from errors or loss of information
C. All instances of data being identical in form content and meaning
D. Data being displayed and stored the same way on all system

**Answer:** C

**NEW QUESTION 197**
Which layer of the OSI layer model is responsible for associate MAC addresses to network devices

A. Physical layer
B. Network layer C Data link layer
C. Transport layer

**Answer:** C

**NEW QUESTION 200**
What is the main purpose of using digital signatures in communication security?

A. To encrypt sensitive data during transmission
B. To verify the identity of the sender and ensure the integrity of the message (Correct)
C. To prevent unauthorized access to a network
D. To compress data to reduce bandwidth usage

**Answer:** B

**NEW QUESTION 205**
What is the primary goal of Identity and Access Management (1AM) in cybersecurity?

A. To ensure 100% security against all threats
B. To provide secure and controlled access to resources
C. To eliminate the need for user authentication
D. To monitor network traffic for performance optimization

**Answer:** A

**NEW QUESTION 207**
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 212**
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 214**
A Company wants to ensure that its employees can access the network resources from anywhere in the world which access control model is best suited for this scenario

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

**Answer:** D

**NEW QUESTION 216**
What is the process of verifying a users identity called?

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

**Answer:** B

**NEW QUESTION 217**
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 218**
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 223**
An organization develops a set of procedures to restore critical business processes after a significant disruption. What type of plan is this?

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

**Answer:** A

**NEW QUESTION 224**
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 228**
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 229**
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 230**
What is sensitivity in the context of confidentiality

A. The harm caused to externl stakeholders if information is disclosed or modified
B. The ability of information to be accessed only by authorized individuals
C. The need for protection assigned to information by its owner
D. The Health status of the individuals

**Answer:** C

**NEW QUESTION 234**
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 237**
A/hich layer of the OSI Layer model is the target of a buffer overflow attack

A. Layer 7
B. Layer 3

C. Layer 5
D. Layer 4

**Answer:** A

**NEW QUESTION 238**
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 243**
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 245**
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 249**
Which of the following protocols is a secure alternative to using telnet?

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

**Answer:** B

**NEW QUESTION 254**
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 258**
Which of the following is the least secure communications protocol?

A. CHAP
B. Ipsec
C. PAP
D. EAP

**Answer:** C

**NEW QUESTION 263**
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 268**
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 269**
Permitting authorized access to information while protecting it from improper disclosure

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

**Answer:** B

**NEW QUESTION 274**
Example of Type 1 Authentication

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

**Answer:** A

**NEW QUESTION 275**
1 _____ is a weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability or set of vulnerabilities.

A. Likelihood of occurrence
B. Threat Vector
C. Risk
D. Impact

**Answer:** A

**NEW QUESTION 278**
Ignoring the risk and proceeding the business operations

A. Risk Acceptance
B. Risk Mitigation
C. Risk Avoidance
D. Risk Transfer

**Answer:** A

**NEW QUESTION 283**
What should been done to limit the damage caused by the ransomware attack

A. Use a different email client to prevent malicious attachments
B. Add more Administrative users to the Domain Admins group
C. Delete all emails with attachments
D. Limit the use of administrative privileges to only when required

**Answer:** D

**NEW QUESTION 288**
A security event, or combination of security events, that constitutes a secu incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization

A. Intrusion
B. Exploit
C. Threat
D. Attack

**Answer:** A

**NEW QUESTION 291**
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 294**
What is the main challenge in achieving non repudiation in electronic transactions

A. Ensuring the identity of the sender and recipient is verified
B. Ensuring the authenticity and integrity of the message
C. Making sure the message is not tampered with during transmission
D. All of the above

**Answer:** D

**NEW QUESTION 295**
An unknown person obtaining access to the company file system without authorization is example of

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

**Answer:** B

**NEW QUESTION 297**
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 300**
In incident terminology the Zero day is

A. Days with a cybersecurity incident
B. A previously unknown system vulnerability
C. Days without a cybersecurity incident
D. Days to solve a previously unknown system vulnerability

**Answer:** B

**NEW QUESTION 305**
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 307**
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 308**
The amount of risk, at a broad level, that an organization is willing to accept in pursuit of its strategic objectives.

A. Risk Assessment
B. Risk Transfer
C. Risk Appetite
D. Risk Management

**Answer:** C

**NEW QUESTION 311**
allows for extremely granular restrictions within the IT environment, to the point where rules can be applied to individual machines and/or users,

A. DMZ
B. Microsegmentation
C. VLAN
D. NAC

**Answer:** B

**NEW QUESTION 312**
Can be considered to be a fingerprint of the file or message

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

**Answer:** A

**NEW QUESTION 316**
When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called _____

A. Malware
B. Zero-day
C. Event
D. Attack

**Answer:** B

**NEW QUESTION 317**
Example of Technical controls

A. Security Guard
B. GPS installed in vehicle to track location
C. Door Lock
D. None

**Answer:** B

**NEW QUESTION 318**
Provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient.

A. Hashing
B. Encoding
C. Cryptography
D. AII

**Answer:** C

**NEW QUESTION 319**
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 324**
A hacker gains access to an organization system without authorization and steal confidential data. What term best describes this ?

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

**Answer:** C

**NEW QUESTION 329**
In which cloud model does the cloud customer have less responsibility over the infrastructure

A. FaaS
B. SaaS
C. laaS
D. PaaS

**Answer:** B

**NEW QUESTION 334**
Which of the following is a common security measure to prevent Cross Site Scripting (XSS) attacks in web applications?

A. implementing strong password policies
B. using a firewall to block incoming traffic
C. validating and sanitizing user input (Correct)
D. encrypting data during transmission

**Answer:** C

**NEW QUESTION 337**
Duke would like to restrict users from accessing a list of prohibited websites while connected to his network. Which one of the following controls would BEST achieve his objective?

A. URL Filter
B. IP Address Block
C. DLP Solution
D. IPS Solution

**Answer:** A

**NEW QUESTION 340**
What does the concept of integrity applied to

A. Organization
B. Information system and processes for business operations
C. People
D. ALL

**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 348**
Which authentication helps build relationships between different technology providers, enabling automatic identification and user access. Employees no longer need to enter separate usernames and passwords when visiting a new service provider

A. Basic
B. Kerberos
C. Token Based
D. Federated

**Answer:** D

**NEW QUESTION 352**
The Order of controls used in Defence in Depth

A. Assests, Physical control
B. Administrative Controls, Logical/Techincal Controls
C. Assests, Administrative Controls, Physical controls, Logical/Techincal Controls
D. Physical control
E. Administrative Controls, Logical/Techincal Controls, Assests
F. Assests, Administrative Controls, Logical/Techincal Controls, Physical controls

**Answer:** D

**NEW QUESTION 354**

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 356**
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 358**
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. AII

**Answer:** C

**NEW QUESTION 363**
Port scanning attack target which OSI layer

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

**Answer:** A

**NEW QUESTION 365**
Four main components of Incident Response are

A. Preparation, Detection and Analysis, Containment, Eradication a
B. Preparation, Detection, Analysis and Containment
C. Detection, Analysis, Containment, Eradication and Recovery
D. AII

**Answer:** A

**NEW QUESTION 369**
Mark works in the security office. During research, Mark learns that a configuration change could better protect the organization's IT environment. Mark makes a proposal for this change, but the change cannot be implemented until it is approved, tested, and then cleared for deployment by the Change Control Board. This is an example of _____

A. Holistic security
B. Defense in depth
C. Threat intelligence
D. Segregation of duties

**Answer:** D

**NEW QUESTION 371**
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 373**
Which of the following is unlikely to be a member of the disaster recovery team

A. Executive Management

B. Public Relations
C. Billing Clerk
D. IT personnel

**Answer:** C

**NEW QUESTION 377**
A backup is which type for security control

A. Preventive
B. Deterrent
C. Recovery
D. Corrective

**Answer:** C

**NEW QUESTION 380**
Token Ring used in which OSI Layer

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

**Answer:** D

**NEW QUESTION 384**
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 386**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CC Product From:

**https://www.2passeasy.com/dumps/CC/**

## Money Back Guarantee

## CC Practice Exam Features:

* CC Questions and Answers Updated Frequently

* CC Practice Questions Verified by Expert Senior Certified Staff

* CC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year