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
In the context of cybersecurity, typical threat actors include the following:

A. Insiders (either deliberately, by simple human error, or by gross incompetence).
B. Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
C. Technology (such as free-running bots and artificial intelligence
D. All

Answer: D

NEW QUESTION 2
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 3
4 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 4
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 5
Common network device used to connect networks?

A. Server
B. Endpoint
C. Router
D. Switch

Answer: C

NEW QUESTION 6
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 7
Which is related to Standard

A. NIST
B. GDPR
C. HIPAA
D. ALL

Answer: A

NEW QUESTION 8
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 9
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 10
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 10
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 11
Which one of the following controls is not particularly effective against the insider threat?

A. Least privilege
B. Background checks
C. Firewalls
D. Separation of duties

Answer: C

NEW QUESTION 13
What is an incident in the context of cybersecurity

A. Any observable occurrence in a network or system
B. A deliberate security incident in which an intruder gains access to a system or system resource without authorization
C. A particular attack that exploits system vulnerabilities
D. An event that actually or potentially jeopardizes the confidentiality integrity or availability of an information system.

Answer: D

NEW QUESTION 15
A cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites

A. Phising
B. Virus
C. Spoofing
D. DDOS

Answer: D

NEW QUESTION 17
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 22
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 27
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 30
What is the difference between BCP and DRP

A. BCP is about restoring IT and communications back to full operations after a disruption, while DRP is about maintaining critical business functions
B. DRP is about restoring IT and communications back to full operations after a disruption, while BCP i about maintaining critical business functions
C. DRP and BCP are the same
D. BCP is about maintaining critical business functions before a disaster occurs

Answer: B

NEW QUESTION 33
Which layer does VLAN hopping belong to?

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

Answer: D

NEW QUESTION 34
What does Personally Identifiable Information (Pll) pertain to?

A. Information about an individual's health status
B. Data about an individual that could be used to identify them (Correct)
C. Trade secrets, research, business plans and intellectual property
D. The importance assigned to information by its owner

Answer: B

NEW QUESTION 37
What security feature used in HTTPS

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

Answer: D

NEW QUESTION 40
The primary functionality of PAM is?

A. Validate the level of access a user have to a file
B. Prevent unauthorized access to organizational assets
C. Provide just-in-time access to critical resources
D. Manage centralized access control

Answer: C

NEW QUESTION 41
Which Prevents Threat

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

Answer: A

NEW QUESTION 46
When Operating in A Cloud Environment, What Cloud Deployment Model Provides Security Teams With The Greatest Access To Forensic Information?

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

Answer: D

NEW QUESTION 47
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 49
What is the purpose of non-repudiation in information security?

A. To ensure data is always accessible when needed
B. To protect data from unauthorized access
C. To prevent the sender or recipient of a message from denying having sent or received the message
D. To ensure data is accurate and unchanged

Answer: C

NEW QUESTION 54
Which is the component of a Business Continuity (BC) plan

A. Immediate response procedures and checklists
B. Notification systems and call trees for alerting personnel
C. Guidance for management, including designation of authority for specific managers
D. ALL

Answer: D

NEW QUESTION 56
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 59
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 60
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 65
Which of the following uses registered port

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

Answer: D

NEW QUESTION 67
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 70
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 75
The magnitude of the harm expected as a result of the consequences of an unauthorized disclosure, modification, destruction or loss of information is known as

A. Threat
B. Vulnerability
C. Impact
D. Likelihood

Answer: C

NEW QUESTION 78
The requirement of both the manager and the accountant to approve the transaction fund exceeding $ 50000. Which security concept best suits this

A. MAC
B. Defence in Depth
C. Two Person integrity
D. Principle of least privilege

Answer: C

NEW QUESTION 82
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 communications back to full operations after the disruptions
D. Guiding the actions of emergency response personnel during the disruption

Answer: C

NEW QUESTION 85
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 86
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 91
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 93
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 95
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 99
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 102
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 106
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 107
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 111
Which plan provides the team with immediate response procedures and check lists and guidance for management?

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

Answer: A

NEW QUESTION 112
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 117
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 119
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 120
Which Prevent crime by designing a physical environment that positively influences human behavior.

A. DMZ
B. Security Alarm
C. CPTED
D. CCTV

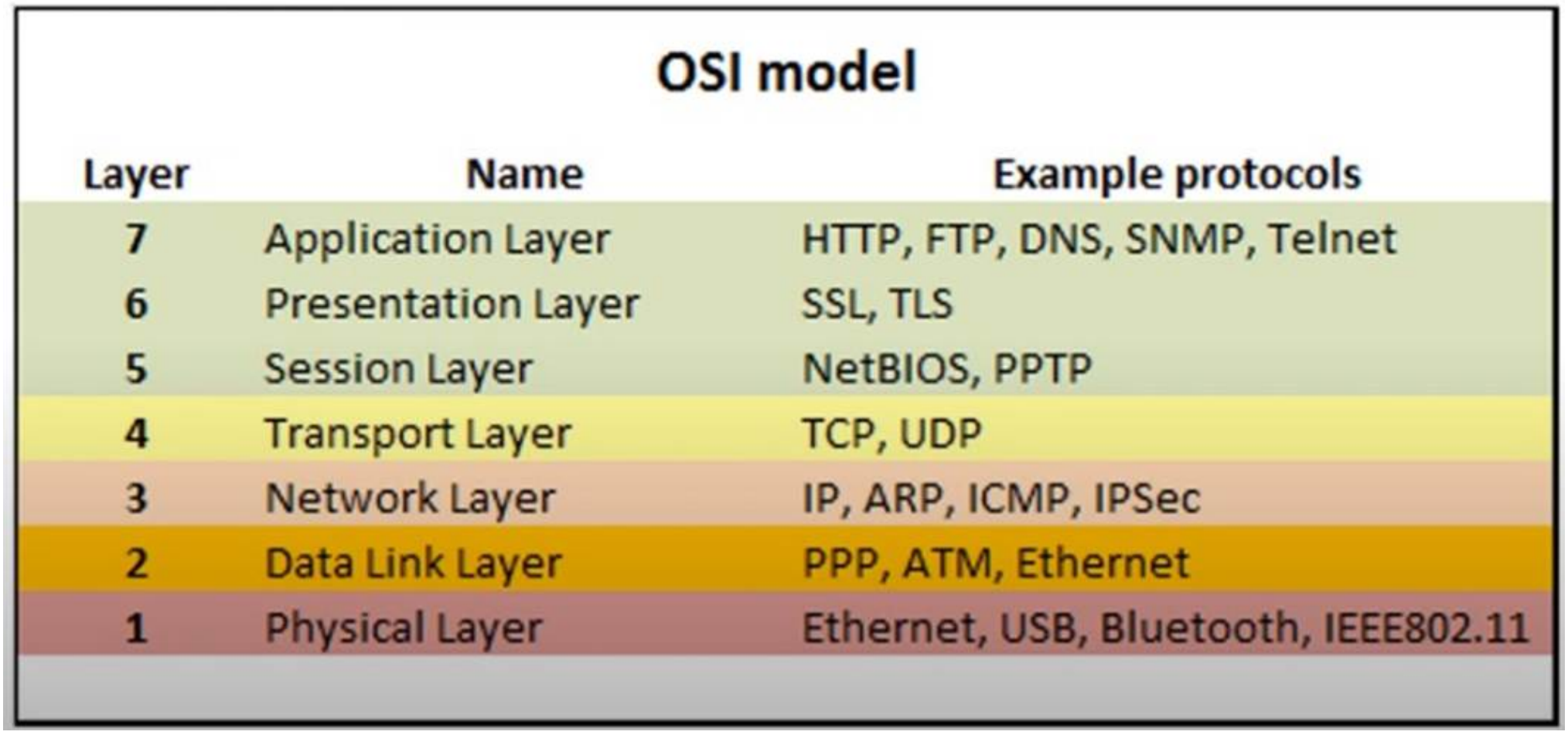
Answer: C

NEW QUESTION 125
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 130
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 132
What is the recommended range of temperature for optimized maximum uptime and hardware life in a data center?

A. 62 F to 69 F
B. 64 F to 81 F
C. 82 F to 90 F
D. 91 F to 100 F

Answer: B

NEW QUESTION 137
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 Analys

Answer: D

NEW QUESTION 141
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 143
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 147
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 148
Sending employees to work at a customer's home can open your business to more risk of bodily injury or property damage claims. So, to reduce risk and avoid potential losses, you decide not to offer those kinds of services

A. Risk Acceptance
B. Risk Assessment
C. Risk Avoidance
D. Risk Control

Answer: C

NEW QUESTION 149
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 154
What is a security token used to authenticate a user to a web application, typically after they log in?

A. Captcha
B. API key
C. CSRF token
D. Session token

Answer: D

NEW QUESTION 155
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 159
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

A. Security Assessment
B. Risk Assessment
C. DRP
D. IRP

Answer: A

NEW QUESTION 164
Which type of malware encrypts a users file system and demands payment in exchange of decrypting key

A. Worm
B. Trojan
C. virus
D. Ransomware

Answer: D

NEW QUESTION 168
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 173
Shaun is planning to protect their data in all states(Rest, Motion, use), defending against data leakage. What would be the BEST solution to implement?

A. End to end encryption.
B. Hashing
C. DLP
D. Threat Modeling

Answer: C

NEW QUESTION 177
Who must follow HIPAA Compliance

A. Energy Sector
B. Health Care
C. Finance Sector
D. ALL

Answer: B

NEW QUESTION 182
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 183
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 185
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 189
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 193
Access control used in in high-security situations such as military and government organizations.

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

Answer: B

NEW QUESTION 198
Restoring IT and communications back to full operation after a disruption.

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

Answer: C

NEW QUESTION 199
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 204
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 209
Granting a user access to services or the system

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

Answer: C

NEW QUESTION 211
Which of the following best describes a zero-day vulnerability?

A. A vulnerability that has been identified and patched by software vendors
B. A vulnerability that has not yet been discovered or publicly disclosed.
C. A vulnerability that can only be exploited by experienced hackers.
D. A vulnerability that affects only legacy systems.

Answer: B

NEW QUESTION 215
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 216
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 221
Which is the first step in the risk management process

A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment

Answer: C

NEW QUESTION 224
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 225
A company experiences a major IT outage and cannot perform its critical business functions. What type of plan will hep the company recover from this event?

A. BCP
B. IRP C DRP
C. BIA

Answer: C

NEW QUESTION 227
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 230
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 233
The highest-level governance documents in an organization, usually approved and issued by management, usually to support a compliance initiative

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

Answer: B

NEW QUESTION 235
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 238
Ignoring the risk and proceeding the business operations

A. Risk Acceptance
B. Risk Mitigation

C. Risk Avoidance
D. Risk Transfer

Answer: A

NEW QUESTION 243
Who is responsible for publishing and signing the organization s policies?

A. The security office
B. Human resources
C. Senior management
D. The legal department

Answer: C

NEW QUESTION 248
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 250
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 252
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 257
A new BYOD policy has been enforced in NEW Corp which type of control is used to enforce thissecurity policies

A. Physical control
B. Logical Control
C. Administrative Control
D. Technical Control

Answer: C

NEW QUESTION 262
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 266
A Hacker launched a specific attack to exploit a known system vulnerability. What term best describes this situation?

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

Answer: C

NEW QUESTION 269
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 274
Walmart has large ecommerce presence in world. Which of these solutions would ensure the LOWEST possible latency for their customers using their services?

A. CDN
B. SaaS
C. Load Balancing
D. Decentralized Data Centers

Answer: A

NEW QUESTION 276
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 281
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 283
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 286
A large organization is planning to create a DRP. Which of the following is the BEST document to provide a high-level overview of the plan?

A. Technical guides for IT personnel
B. Department specific plans
C. Full copies of the plan for critical disaster recovery team members
D. Execute summary

Answer: D

NEW QUESTION 289
Government can imposes financial penalties as a consequence of breaking a

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

Answer: B

NEW QUESTION 291
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 292
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 297
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 302
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 305
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 306
Which one of the following groups is NOT normally part of an organization's cybersecurity incident response team?

A. Technical Subject Matter Experts
B. Cybersecurity Experts
C. Management
D. Law Enforcement

Answer: D

NEW QUESTION 309
Is the right of an individual to control the distribution of information about themselves

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

Answer: C

NEW QUESTION 310
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 313
Which is not possible models for an Incident Response Team (IRT):

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

Answer: D

NEW QUESTION 316
Uses multiple types of access controls in literal or theoretical layers to help an organization avoid a monolithic security

A. DMZ
B. VLAN
C. Defence in Depth
D. VPN

Answer: C

NEW QUESTION 319
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 323
A standard that defines wired communications of network devices

A. Switch
B. Hub
C. router
D. Ethernet

Answer: D

NEW QUESTION 326
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 327
Token Ring used in which OSI Layer

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

Answer: D

NEW QUESTION 332
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 334

.....

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/