ISC2

Certified in Cybersecurity (CC)

QUESTION

Collected By: Ayemun Hossain

Question: 1

The address 8be2:4382:8d84:7ce2:ec0f:3908:d29a:903a is an:

A. Web address

B. IPv4 address

C. IPv6 address

D. Mac address

Question: 2

Which of the following canons is found in the ISC2 code of ethics?

A. Advance and promote the profession

B. Protect society, the common good, and the infrastructure

C. Provide diligent and competent service to principals

D. Act honorably, honestly, safely and legally

Question: 3

Which of the following is NOT an ethical canon of the ISC2?

A. Advance and protect the profession

B. Protect society, the common good, necessary public trust and confidence, and the infrastructure

C. Act honorably, honestly, justly, responsibly and legally

D. Provide active and qualified service to principal

Question: 4

The cloud deployment model where a company has resources on-premise and in the cloud is known as:

A. Hybrid cloud

B. Multi-tenant

C. Private cloud

D. Community cloud

Question: 5

Which of the following is a public IP?

A. 13.16.123.1

B. 192.168.123.1

C. 172.16.123.1

D. 10.221.123.1

Explanation/Reference:

The ranges of IP addresses 10.0.0.0 to 10.255.255.254, 172.16.0.0 to 172.31.255.254, and 192.168.0.0 to 192.168.255.254 are reserved for private use (see ISC2 Study Guide, chapter 4, module 1, under Internet Protocol - IPv4 and IPv6). Therefore, the IP address 13.16.123.1 is the only address in a public range.

Question: 6

Which of the following is a data handling policy procedure?

A. Transform

B. Collect

C. Encode

D. Destroy

Question: 7

Which devices would be more effective in detecting an intrusion into a network?

A. Routers

B. HIDS

C. Firewalls

D. NIDS

:

Question: 8

Which concept describes an information security strategy that integrates people, technology and operations in order to establish security controls across multiple layers of the organization?

A. Least Privilege

B. Defense in Depth

C. Separation of Duties

D. Privileged Accounts

Question: 9

Which access control is more effective at protecting a door against unauthorized access?

A. Fences

B. Turnstiles

C. Barriers

D. Locks

:

Question: 10

Which of the following is a detection control?

A. Turnstiles

B. Smoke sensors

C. Bollards

D. Firewalls

Question: 11

Which type of attack has the PRIMARY objective controlling the system from outside?

A. Backdoors

B. Rootkits

C. Cross-Site Scripting

D. Trojans

Question: 12

Which of the following is not a protocol of the OSI Level 3?

A. SNMP

B. ICMP

C. IGMP

D. IP

Question: 13

When a company hires an insurance company to mitigate risk, which risk management technique is being applied?

A. Risk avoidance

B. Risk transfer

C. Risk mitigation

D. Risk tolerance

Question: 14

The SMTP protocol operates at OSI Level:

A. 7

B. 25

C. 3

D. 23

Question: 15

The process of verifying or proving the user's identification is known as:

A. Confidentiality

B. Integrity

C. Authentication

D. Authorization

Question: 16

If an organization wants to protect itself against tailgating, which of the following types of access control would be most effective?

A. Locks

B. Fences

C. Barriers

D. Turnstiles

Question: 17

Logging and monitoring systems are essential to:

A. Identifying inefficient performing systems, preventing compromises, and providing a record of how systems are used

B. Identifying efficient performing systems, labeling compromises, and providing a record of how systems are used

C. Identifying inefficient performing systems, detecting compromises, and providing a record of how systems are used

D. Identifying efficient performing systems, detecting compromises, and providing a record of how systems are used

Question: 18

In the event of a disaster, which of these should be the PRIMARY objective? (★)

A. Guarantee the safety of people

B. Guarantee the continuity of critical systems

C. Protection of the production database

D. Application of disaster communication

Question: 19

The process that ensures that system changes do not adversely impact business operations is known as:

A. Change Management

B. Vulnerability Management

C. Configuration Management

D. Inventory Management

Question: 20

The last phase in the data security cycle is:

A. Encryption

B. Backup

C. Archival

D. Destruction

Question: 21

Which access control model specifies access to an object based on the subject's role in the organization?

A. RBAC

B. MAC

C. DAC

D. ABAC

Question: 22

Which of the following is NOT an example of a physical security control?

A. Firewalls

B. Biometric access controls

C. Remote control electronic locks

D. Security cameras

Question: 23

Which type of attack will most effectively maintain remote access and control over the victim's computer?

A. Trojans

B. Phishing

C. Cross-Site Scripting

D. Rootkits

Question: 24

In incident terminology, the meaning of Zero Day is:

A. Days to solve a previously unknown system vulnerability

B. A previously unknown system vulnerability

C. Days without a cybersecurity incident

D. Days with a cybersecurity incident

Question: 25

Which of the following is NOT a possible model for an Incident Response Team (IRT)?

A. Leveraged

B. Pre-existing

C. Dedicated

D. Hybrid

Explanation/Reference:

The three possible models for incident response are Leveraged, Dedicated, and Hybrid (see the ISC2 Study Guide, Chapter 2, Module 1, under Chapter Takeaways). The term 'Pre-existing' is not a valid model for an IRT.

Question: 26

A device found not to comply with the security baseline should be:

A. Disabled or separated into a quarantine area until a virus scan can be run

B. Disabled or isolated into a quarantine area until it can be checked and updated.

C. Placed in a demilitarized zone (DMZ) until it can be reviewed and updated

D. Marked as potentially vulnerable and placed in a quarantine area

Question: 27

A biometric reader that grants access to a computer system in a data center is a:

A. Administrative Control

B. Physical Control

C. Authorization Control

D. Technical Control

Question: 28

Which type of attack PRIMARILY aims to make a resource inaccessible to its intended users?

A. Denials of Service

B. Phishing

C. Trojans

D. Cross-Site Scripting

Question: 29

Which type of attack embeds malicious payload inside a reputable or trusted software?

A. Trojans

B. Phishing

C. Rootkits

D. Cross-Site Scripting

Question: 30

Which tool is commonly used to sniff network traffic? (★)

A. Burp Suite

B. John the Ripper

C. Wireshark

D. Nslookup

Question: 31

Which of these is not an attack against an IP network?

A. Side-channel Attack

B. Man-in-the-middle Attack

C. Fragmented Packet Attack

D. Oversized Packet Attack

Question: 32

The detailed steps to complete tasks supporting departmental or organizational policies are typically documented in:

A. Regulations

B. Standards

C. Policies

D. Procedures

Question: 33

Which device is used to connect a LAN to the Internet?

A. SIEM

B. HIDS

C. Router

D. Firewall

Question: 34

What does SIEM mean?

A. Security Information and Enterprise Manager

B. Security Information and Event Manager

C. System Information and Enterprise Manager

D. System Information and Event Manager

Question: 35

A Security safeguard is the same as a:

A. Safety control

B. Privacy control

C. Security control

D. Security principle

Question: 36

Which access control model can grant access to a given object based on complex rules?

A. DAC

B. ABAC

C. RBAC

D. MAC

Question: 37

Which port is used to secure communication over the web (HTTPS)?

A. 69

B. 80

C. 25

D. 443

Question: 38

Which of these has the PRIMARY objective of identifying and prioritizing critical business processes?

A. Business Impact Plan

B. Business Impact Analysis

C. Disaster Recovery Plan

D. Business Continuity Plan

Question: 39

Which of the following are NOT types of security controls?

A. Common controls

B. Hybrid controls

C. System-specific controls

D. Storage controls

Question: 40

Which of the following is NOT a type of learning activity used in Security Awareness?

A. Awareness

B. Training

C. Education

D. Tutorial

Question: 41

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 the:

A. Vulnerability

B. Threat

C. Impact

D. Likelihood

Question: 42

The implementation of Security Controls is a form of:

A. Risk reduction

B. Risk acceptance

C. Risk avoidance

D. Risk transference

Question: 43

Which of the following attacks take advantage of poor input validation in websites?

A. Trojans

B. Cross-Site Scripting

C. Phishing

D. Rootkits

.

Question: 44

Which of the following is an example of an administrative security control?

A. Access Control Lists

B. Acceptable Use Policies

C. Badge Readers

D. No entry signs

Question: 45

In Change Management, which component addresses the procedures needed to undo changes?

A. Request for Approval

B. Request for Change

C. Rollback

D. Disaster and Recover

Question: 46

Which of the following properties is NOT guaranteed by Digital Signatures?

A. Authentication

B. Confidentiality

C. Non-Repudiation

D. Integrity

Question: 47

Which devices have the PRIMARY objective of collecting and analyzing security events?

A. Hubs

B. Firewalls

C. Routers

D. SIEM

Question: 48

What is an effective way of hardening a system?

A. Patch the system

B. Have an IDS in place

C. Run a vulnerability scan

D. Create a DMZ for web application services

Question: 49

Which type of key can be used to both encrypt and decrypt the same message?

A. A public key

B. A private key

C. An asymmetric key

D. A symmetric key

Question: 50

Which regulations address data protection and privacy in Europe?

A. SOX

B. HIPAA

C. FISMA

D. GDPR

Question: 51

Which of the following types of devices inspect packet header information to either allow or deny network traffic?

A. Hubs

B. Firewalls

C. Routers

D. Switches

Question: 52

A web server that accepts requests from external clients should be placed in which network?

A. Intranet

B. DMZ

C. Internal Network

D. VPN

Question: 53

Sensitivity is a measure of the …:

A. … protection and timeliness assigned to information by its owner, or the purpose of representing its need for urgency.

B. … urgency and protection assigned to information by its owner.

C. … importance assigned to information by its owner, or the purpose of representing its need for protection.

D. … pertinence assigned to information by its owner, or the purpose of representing its need for urgency.

Question: 54

How many data labels are considered good practice?

A. 2 - 3

B. 1

C. 1-2

D. >4

Question: 55

Security posters are an element PRIMARILY employed in: (★)

A. Security Awareness

B. Incident Response Plans

C. Business Continuity Plans

D. Physical Security Controls

Question: 56

Which of these types of user is LESS likely to have a privileged account?

A. System Administrator

B. Security Analyst

C. Help Desk

D. External Worker

Question: 57

Which of the following is NOT an element of System Security Configuration Management?

A. Inventory

B. Baselines

C. Updates

D. Audit logs

Question: 58

Which are the components of an incident response plan?

A. Preparation -> Detection and Analysis -> Recovery -> Containment -> Eradication -> Post-Incident Activity

B. Preparation -> Detection and Analysis -> Containment -> Eradication -> Post-Incident Activity -> Recovery

C. Preparation -> Detection and Analysis -> Eradication -> Recovery -> Containment -> Post-Incident Activity

D. Preparation -> Detection and Analysis -> Containment, Eradication and Recovery -> Post-Incident Activity

Question: 59

Which of the following is an example of 2FA?

A. Badges

B. Passwords

C. Keys

D. One-Time passwords (OTA)

Question: 60

The predetermined set of instructions or procedures to sustain business operations after a disaster is commonly known as:

A. Business Impact Analysis

B. Disaster Recovery Plan

C. Business Impact Plan

D. Business Continuity Plan

Question: 61

Which of the following is NOT a feature of a cryptographic hash function?

A. Reversible

B. Unique

C. Deterministic

D. Useful

Question: 62

Which are the three packets used on the TCP connection handshake? (★)

A. Offer → Request → ACK

B. SYN → SYN/ACK → ACK

C. SYN → ACK → FIN

D. Discover → Offer → Request

Question: 63

After an earthquake disrupting business operations, which document contains the procedures required to return business

to normal operation?

A. The Business Impact Plan

B. The Business Impact Analysis

C. The Business Continuity Plan

D. The Disaster Recovery Plan

Question: 64

What is the consequence of a Denial Of Service attack?

A. Exhaustion of device resources

B. Malware Infection

C. Increase in the availability of resources

D. Remote control of a device

Question: 65

According to ISC2, which are the six phases of data handling?

A. Create -> Use -> Store -> Share -> Archive -> Destroy

B. Create -> Store -> Use -> Share -> Archive -> Destroy

C. Create -> Share -> Use ->Store -> Archive -> Destroy

D. Create -> Share -> Store -> Use -> Archive -> Destroy

Question: 66

Which of the following is less likely to be part of an incident response team?

A. Legal representatives

B. Human Resources

C. Representatives of senior management

D. Information security professionals

Question: 67

Which of these tools is commonly used to crack passwords? (★)

A. Burp Suite

B. Nslookup

C. John the Ripper

D. Wireshark

Question: 68

In order to find out whether personal tablet devices are allowed in the office, which of the following policies would be helpful to read?

A. BYOD

B. Privacy Policy

C. Change Management Policy

D. AUP

Question: 69

In which cloud deployment model do companies share resources and infrastructure on the cloud?

A. Hybrid cloud

B. Multi-tenant

C. Private cloud

D. Community cloud

Question: 70

Which of these is the PRIMARY objective of a Disaster Recovery Plan?

A. Restore company operation to the last-known reliable operation state

B. Outline a safe escape procedure for the organization's personnel

C. Maintain crucial company operations in the event of a disaster

D. Communicate to the responsible entities the damage caused to operations in the event of a disaster

Question: 71

An entity that acts to exploit a target organization's system vulnerabilities is a:

A. Threat Vector

B. Threat Actor

C. Threat

D. Attacker

Question: 72

A best practice of patch management is to:

A. Apply all patches as quickly as possible

B. Test patches before applying them

C. Apply patches every Wednesday

D. Apply patches according to the vendor's reputation

Question: 73

Which of these would be the best option if a network administrator needs to control access to a network?

A. HIDS

B. IDS

C. SIEM

D. NAC

Question: 74

Which of these is NOT a change management component?

A. Approval

B. RFC

C. Rollback

D. Governance

Question: 75

Which of the following is NOT a social engineering technique?

A. Pretexting

B. Quid pro quo

C. Double-dealing

D. Baiting

Question: 76

If there is no time constraint, which protocol should be employed to establish a reliable connection between two devices?

A. TCP

B. DHCP

C. SNMP

D. UDP

Question: 77

An exploitable weakness or flaw in a system or component is a:

A. Threat

B. Bug

C. Vulnerability

D. Risk

Question: 78

In which cloud model does the cloud customer have LESS responsibility over the infrastructure? (★)

A. IaaS

B. FaaS

C. PaaS

D. SaaS

Question: 79

Risk Management is:

A. The assessment of the potential impact of a threat.

B. The creation of an incident response team.

C. The impact and likelihood of a threat.

D. The identification, evaluation and prioritization of risks.

Question: 80

Which of the following documents contains elements that are NOT mandatory?

A. Policies

B. Guidelines

C. Regulations

D. Procedures

Question: 81

In which of the following phases of an Incident Recovery Plan are incident responses prioritized?

A. Post-incident Activity

B. Detection and Analysis

C. Preparation

D. Contentment, Eradication, and Recovery

Question: 82

Which security principle states that a user should only have the necessary permission to execute a task?

A. Privileged Accounts

B. Separation of Duties

C. Least Privilege

D. Defense in Depth

Question: 83

The Bell and LaPadula access control model is a form of: (★)

A. ABAC

B. RBAC

C. MAC

D. DAC

Question: 84

In risk management, the highest priority is given to a risk where:

A. The frequency of occurrence is low, and the expected impact value is high

B. The expected probability of occurrence is low, and the potential impact is low

C. The expected probability of occurrence is high, and the potential impact is low

D. The frequency of occurrence is high, and the expected impact value is low

Question: 85

Which of the following areas is connected to PII?

A. Non-Repudiation

B. Authentication

C. Integrity

D. Confidentiality

Question: 86

According to the canon "Provide diligent and competent service to principals", ISC2 professionals are to:

A. Take care not to tarnish the reputation of other professionals through malice or indifference.

B. Treat all members fairly and,when resolving conflicts, consider public safety and duties to principals, individuals and the profession, in that order.

C. Avoid apparent or actual conflicts of interest.

D. Promote the understanding and acceptance of prudent information security measures.

Question: 87

Malicious emails that aim to attack company executives are an example of:

A. Trojans

B. Whaling

C. Phishing

D. Rootkits

Question: 88

Governments can impose financial penalties as a consequence of breaking a:

A. Regulation

B. Standard

C. Policy

D. Procedure

Question: 89

Which type of attack attempts to trick the user into revealing personal information by sending a fraudulent message?

A. Phishing

B. Cross-Site Scripting

C. Denials of Service

D. Trojans

Question: 90

In which of the following access control models can the creator of an object delegate permission?

A. ABAC

B. MAC

C. RBAC

D. DAC

Question: 91

Which type of attack has the PRIMARY objective of encrypting devices and their data, and then demanding a ransom payment for the decryption key?

A. Ransomware

B. Trojan

C. Cross-Site Scripting

D. Phishing

Question: 92

Which of the following cloud models allows access to fundamental computer resources? (★)

A. SaaS

B. FaaS

C. PaaS

D. IaaS

Question: 93

How many layers does the OSI model have?

A. 7

B. 4

C. 6

D. 5

Question: 94

Which of the following principles aims primarily at fraud detection?

A. Privileged Accounts

B. Defense in Depth

C. Least Privilege

D. Separation of Duties

Question: 95

Which protocol uses a three-way handshake to establish a reliable connection?

A. TCP

B. SMTP

C. UDP

D. SNMP

Question: 96

Which of the following is an example of a technical security control?

A. Access control lists

B. Turnstiles

C. Fences

D. Bollards

Question: 97

Which type of attack attempts to gain information by observing the device's power consumption? (★)

A. Side Channels

B. Trojans

C. Cross Site Scripting

D. Denials of Service

Question: 98

Which of the following areas is the most distinctive property of PHI?

A. Integrity

B. Confidentiality

C. Non-Repudiation

D. Authentication

Question: 99

Which of these is the most efficient and effective way to test a business continuity plan?

A. Simulations

B. Walkthroughs

C. Reviews

D. Discussions

Question: 100

Which of the following Cybersecurity concepts guarantees that information is accessible only to those authorized to access it?

A. Confidentiality

B. Non-repudiation

C. Authentication

D. Accessibility

Question: 101

In the event of a disaster, what should be the PRIMARY objective? (★)

A. Apply disaster communication

B. Protect the production database

C. Guarantee the safety of people

D. Guarantee the continuity of critical systems

Explanation/Reference:

In the event of a disaster, the number one priority is to guarantee the safety of human life above all else. The remaining options, though important as concerns business continuity, are never as important as the safety of human beings.

Question: 102

A security professional should report violations of a company's security policy to:

A. The ISC Ethics Committee

B. Company management

C. National authorities

D. A court of law

Question: 103

Which department in a company is NOT regularly involved in a DRP?

A. Executives

B. IT

C. Public Relations

D. Financial

Question: 104

Which of the following is included in an SLA document?

A. A plan to prepare the organization for the continuation of critical business functions

B. A plan to keep business operations going while recovering from a significant disruption

C. Instructions to detect, respond to, and limit the consequences of a cyber-attack

D. Instructions on data ownership and destruction

Question: 105

What is the most important difference between MAC and DAC?

A. In MAC, security administrators set the roles for the users; in DAC, roles are set at the object owner's discretion

B. In MAC, security administrators assign access permissions; in DAC, security administrators set user roles

C. In MAC, security administrators assign access permissions; in DAC, access permissions are set at the object owner's discretion

D. In MAC, access permissions are set at the object owner's discretion; in DAC, it is up to security administrators to assign access permissions

Question: 106

Requiring a specific user role to access resources is an example of:

A. MAC

B. ABAC

C. RBAC

D. DAC

Question: 107

Which type of document outlines the procedures ensuring that vital company systems keep running during business-disrupting events?

A. Business Impact Plan

B. Business Impact Analysis

C. Disaster Recovery Plan

D. Business Continuity Plan

Question: 108

Which of the following is NOT a best practice in access management?

A. Give only the right amount of permission

B. Periodically assess if user permissions still apply

C. Request a justification when upgrading permission

D. Trust but verify

Question: 109

If a company collects PII, which policy is required?

A. Remote Access Policy

B. GDPR

C. Privacy Policy

D. Acceptable Use Policy

Question: 110

Which of these is LEAST likely to be installed by an infection?

A. Logic Bomb

B. Keylogger

C. Trojan

D. Backdoor

Question: 111

(★) The best defense method to stop a 'Replay Attack' is to:

A. Use an IPSec VPN

B. Use a Firewall

C. Use password authentication

D. Use message digesting

Question: 112

Which of these devices has the PRIMARILY objective of determining the most efficient path for the traffic to flow across the networks?

A. Hubs

B. Firewalls

C. Routers

D. Switches

Question: 113

Which of these types of malware self-replicates without the need for human intervention?

A. Worm

B. Trojan

C. Virus

D. Rootkits

Question: 114

As an (ISC)² member, you are expected to perform with due care. What does 'due care' specifically mean?

A. Do what is right in each situation you encounter on the job

B. Give continuity to the legacy of security practices of your company

C. Apply patches annually

D. Researching and acquiring the knowledge to do your job right

Question: 115

(★) Which of these is NOT a best practice in access management?

A. Periodically assessing whether user permissions still apply

B. Requesting a justification when upgrading permission

C. Giving only the right amount of permission

D. Trust but verify

Question: 116

During the investigation of an incident, which security policies are more likely to cause difficulties?

A. Configuration standards

B. Incident response policies

C. Communication policies

D. Retention policies

Question: 117

In an Access Control List (ACL), the element that determines which permissions you have is:

A. The subject

B. The object

C. The firmware

D. The rule

Question: 118

What does the term 'data remanence' refer?

A. Data in use that can't be encrypted

B. Files saved locally that can't be remoted accessed

C. Data left over after routine removal and deletion

D. All of the data in a system

Question: 119

(★) Which type of recovery site has some or most systems in place, but does not have the data needed to take over operations?

A. A hot site

B. A cloud site

C. A warm site

D. A cold site

Question: 120

Which of these is NOT a characteristic of an MSP implementation?

A. Manage all in-house company infrastructure

B. Monitor and respond to security incidents

C. Mediate, execute and decide top-level decisions

D. Utilize expertise for the implementation of a product or service

Question: 121

Which of these is NOT a typical component of a comprehensive business continuity plan (BCP)?

A. A cost prediction of the immediate response procedures

B. Immediate response procedures and checklists

C. Notification systems and call trees for alerting personnel

D. A list of the BCP team members

Question: 122

Acting ethically is mandatory for (ISC)² members. Which of these is NOT considered unethical?

A. Disrupting the intended use of the internet

B. Seeking to gain unauthorized access to resources on thae internet

C. Compromising the privacy of users

D. Having fake social media profiles and accounts

Question: 123

In an incident response process, which phase uses indicators of compromise and log analysis as part of a review of events?

A. Preparation

B. Eradication

C. Identification

D. Containment

Question: 124

Which of these Access Control Systems is commonly used in the military?

A. ABAC

B. DAC

C. RBAC

D. MAC

Question: 125

Which of these is NOT a security principle?

A. Security in Depth (SID)

B. Zero Trust model

C. Least Privilege

D. Separation of Duties

Question: 126

Which of these is not a common goal of a cybersecurity attacker?

A. Allocation

B. Alteration

C. Disclosure

D. Denial

Question: 127

Which of these types of layers is NOT part of the TCP/IP model?

A. Application

B. Physical

C. Internet

D. Transport

Question: 128

On a BYOD model, which of these technologies is best suited to keep corporate data and applications separate from personal?

A. Biometrics

B. Full-device encryption

C. Context-aware authentication

D. Containerization

Question: 129

In the context of risk management, which information does ALE outline?

A. The expected cost per year of not performing a given risk-mitigating action

B. The business impact of a risk

C. The percentage of Asset Lost Efficiency

D. The probability of a risk coming to pass in a given year

Question: 130

Which of these techniques is PRIMARILY used to ensure data integrity?

A. Message Digest

B. Content Encryption

C. Backups

D. Hashing

Question: 131

Which of these is an example of a privacy breach?

A. Any observable occurrence in a network or system

B. Being exposed to the possibility of attack

C. Unavailability of critical systems

D. Access of private information by an unauthorized person

Question: 132

Which of these terms refers to a collection of fixes?

A. Downgrade

B. Patch

C. Service Pack

D. Hotfix

Question: 133

While performing background checks on new employees, which of these can NEVER be an attribute for discrimination?

A. Employment history, references, criminal records

B. Credit history, employment history, references

C. Criminal Records, credit history, references

D. References, education, political affiliation, employment history

Question: 134

When looking for cybersecurity insurance, which of these is the MOST IMPORTANT objective?

A. Risk acceptance

B. Risk transference

C. Risk avoidance

D. Risk spreading

Question: 135

Which of these documents is MORE directly related to what can be done with a system or with its information?

A. SLA

B. MOA

C. MOU

D. ROE

Question: 136

Which kind of document outlines the procedures ensuring that vital company systems keep running during business-disrupting events?

A. Business Impact Analysis

B. Business Impact Plan

C. Business Continuity Plan

D. Disaster Recovery Plan

Question: 137

Which of these social engineering attacks sends emails that target specific individuals?

A. Pharming

B. Whaling

C. Vishing

D. Spear phishing

Question: 138

(★) Which of these properties is NOT guaranteed by a Message Authentication Code (MAC)?

A. Authenticity

B. Anonymity

C. Integrity

D. Non-repudiation

Question: 139

What is the PRIMARY objective of a degaussing?

A. Preventing magnetic side-channel attacks

B. Reducing noisy data on a disk

C. Erasing the data on a disk

D. Retaining the data on a disk

Question: 140

Which of these is part of the canons (ISC)² code of ethics?

A. Provide diligent and competent services to stakeholders

B. Advance and protect the profession

C. Prevent and detect unauthorized use of digital assets in a society

D. Act always in the best interest of your client

Question: 141

Which of these is NOT one of the (ISC)² ethics canons?

A. Act honorably, honestly, justly, responsibly, and legally

B. Consider the social consequences of the systems you are designing

C. Protect society, the common good, necessary public trust and confidence, and the infrastructure

D. Provide diligent and competent service to principals

Question: 142

(★) Which of these is the PRIMARY objective of the PCI-DSS standard?

A. Personally Identifiable Information (PII)

B. Change Management

C. Secure Credit Cards Payments

D. Protected Health Information (PHI)

Question: 143

Which of these is an attack that encrypts the organization's information, and then demands payment for the decryption code?

A. Phishing

B. DDoS

C. Spoofing

D. Ransomware

Question: 144

The PRIMARY objective of a business continuity plan is:

A. To regularly verify whether the organization complies with applicable regulations

B. To sustain business operations while recovering from a disruption

C. To assess the impact of disruption to the business

D. To restore the business to the full last-known reliable state of operations

Question: 145

Which of these is an attack whose PRIMARY goal is to gain access to a target system through falsified identity?

A. Ransomware

B. Amplification

C. Spoofing

D. DDoS

Question: 146

When an incident occurs, which of these is not a PRIMARY responsibility of an organization's response team?

A. Determining the scope of the damage caused by the incident

B. Implementing the recovery procedures necessary to restore security and recover from any incident-related damage

C. Determining whether any confidential information has been compromised over the course of the entire incident

D. Communicating with top management regarding the circumstances of the cybersecurity event

Question: 147

What is the PRIMARY objective of a rollback in the context of the change management process?

A. Identify the required changes needed

B. Validate the system change process

C. Restore the system to its last state before the change was made

D. Establish a minimum understood and acceptable level of security requirements

Question: 148

Which of these entities is responsible for signing an organization's policies?

A. Human Resources

B. Security engineer

C. Financial Department

D. Senior management

Question: 149

Which of these terms refers to threats with unusually high technical and operational sophistication, spanning months or even years?

A. Rootkit

B. APT

C. Side-channel

D. Ping of death

.

Question: 150

The PRIMARY objective of a security baseline is to establish ...

A. . a minimum understood and a good level of security requirements

B.a minimum understood and acceptable level of security requirements

C. security and configuration requirements

D. a maximum understood and an acceptable level of security requirements

Question: 151

Which of these attacks take advantage of inadequate input validation in websites?

A. Phishing

B. Trojans

C. Cross-Site Scripting

D. Rootkits

Question: 152

An organization needs a network security tool that detects and acts in the event of malicious activity. Which of these tools will BEST meet their needs?

A. Router

B. IPS

C. IDS

D. Firewall

Question: 153

In a DAC policy scenario, which of these tasks can only be performed by a subject granted access to information?

A. Changing security attributes

B. Reading the information

C. Executing the information

D. Modifying the information

Question: 154

In the event of non-compliance, which of these can have considerable financial consequences for an organization?

A. Policies

B. Regulations

C. Guidelines

D. Standards

Question: 155

What does the term LAN refer to?

A. A tool to manage and control network traffic, as well as to protect a network.

B. A network on a building or limited geographical area

C. A device that connects multiple other devices in a network

D. A long-distance connection between geographically-distant networks

Question: 156

Which of these is a type of corrective security control?

A. Patches

B. Intrusion detection systems

C. Guidelines

D. Encryption

Question: 157

Which of these enables point-to-point online communication over an untrusted network?

A. VLAN

B. Firewall

C. Router

D. VPN

Question: 158

At which of the OSI layers do TCP and UDP work?

A. Transport Layer

B. Session Layer

C. Application Layer

D. Physical Layer

Question: 159

(★) Which is the PRIMARY focus of the ISO 27002 standard?

A. Health Insurance Portability and Accountability Act (HIPAA)

B. Information Security Management System (ISMS)

C. Risk Management

D. Application Security

of healthcare information.

Question: 160

(★) Which of these different sub-masks will allow 30 hosts?

A. /26

B. /30

C. /27

D. /29

Question: 161

(★) Which of these statements about the security implications of IPv6 is NOT true?

A. Rules based on static IPv6 addresses may not work

B. IPv6's NAT implementation is insecure

C. IPv6 traffic may bypass existing security controls

D. IPv6 reputation services may not be mature and useful

module 3).

Question: 162

Which of these is a type of detective access control?

A. Bollards

B. Movement Sensors

C. Turnstiles

D. Firewalls

Question: 163

The name, age, location and job title of a person are all examples of:

A. Biometric factors

B. Attributes

C. Account permissions

D. Identity factors

Question: 164

Which cloud service model provides the most suitable environment for customers who want to install their custom operating system?

A. SaaS

B. SLA

C. IaaS

D. PaaS

Question: 165

(★) Which of these statements is TRUE about cybersquatting?

A. Its an unethical practice but everyone does it

B. It is partially illegal practice

C. It is an illegal practice

D. It is s a legal practice

Question: 166

Which of these addresses is commonly reserved specifically for broadcasting?

A. 192.299.121.254

B. 192.299.121.0

C. 192.299.121.14

D. 192.299.121.255

Question: 167

Which department in a company is NOT typically involved in a Disaster Recovery Plan (DRP)?

A. Executive

B. Financial

C. Public Relations

D. IT

Question: 168

Which of these pairs does NOT constitute Multi-Factor Authentication (MFA)?

A. Fingerprint and password.

B. Username and retina scan.

C. Password and username.

D. PIN and credit card.

Question: 169

Which method is COMMONLY used to map live hosts in the network?

A. Geolocation

B. Traceroute

C. Ping sweep

D. Wireshark

Question: 170

A poster reminding the best password management practices is an example of which type of learning activity?

A. Awareness

B. Schooling

C. Education

D. Training

Question: 171

Which part of the CIA Triad will be PRIMARILY jeopardized in a Distributed Denial Of Service (DDOS) attack?

A. Accountability

B. Availability

C. Integrity

D. Confidentiality

Question: 172

(★) What technology is MOST LIKELY to conserve the storage space required for video recordings?

A. Motion detection

B. PTZ

C. Facial recognition

D. Infrared cameras

Question: 173

An organization that uses a layered approach when designing its security architecture is using which of these security approaches?

A. Zero trust

B. Defense in depth

C. Network Layers

D. Network Control Access

Question: 174

Which of these techniques will ensure the property of 'non-repudiation'?

A. Using a VPN

B. Passwords

C. Encryption

D. Digital signatures

Question: 175

(★) A USB pen with data passed around the office is an example of:

A. Data in motion

B. Data at rest

C. Data in transit

D. Data in use

Question: 176

Suppose that an organization wants to implement measures to strengthen its detective access controls. Which one of these tools should they implement?

A. Patches

B. Encryption

C. IDS

D. Backups

Question: 177

(★) Which of these is an example of a MAC address?

A. 00-51-02-1F-58-F6

B. 0051021f58

C. 10.23.19.49

D. 2001 : db8: 3333 : 4444 : 5555 : 6666 : 7777 : 8888

Question: 178

Which of these types of credentials is NOT used in multi-factor authentication?

A. Something you have

B. Something you know

C. Something you are

D. Something you trust

Question: 179

On an Incident Response team, which role acts as the team's main link to Senior Management?

A. Information security

B. Communications and public relations

C. Management

D. Technical expert

Question: 180

Which of these is NOT an effective way to protect an organization from cybercriminals?

A. Removing or disabling unneeded services and protocols

B. Using firewalls

C. Using out-dated anti-malware software

D. Using intrusion detection and prevention systems

Question: 181

Which of these CANNOT be a corrective security control?

A. Disaster Recovery Plan

B. Backups

C. Patches

D. Bollards

Question: 182

Which of these is included in an SLA document?

A. Instructions on data ownership and destruction

B. Instructions to detect, respond to, and limit the consequences of a cyber-attack

C. A plan to keep business operations going while recovering from a significant disruption

D. A plan to prepare the organization for the continuation of critical business functions

Question: 183

Which port number corresponds to the Simple Mail Transfer Protocol (SMTP)?

A. 161

B. 69

C. 25

D. 22

Question: 184

Which type of attack attempts to mislead the user into exposing personal information by sending fraudulent emails?

A. Cross-Site Scripting

B. Denial of Service

C. Trojans

D. Phishing

Question: 185

Which of these is NOT a characteristic of the cloud?

A. Zero Customer Responsibility

B. Broad Network Access

C. Measured Service

D. Rapid Elasticity

Question: 186

Which of these is a COMMON mistake made when implementing record retention policies?

A. Not categorizing the type of information to be retained

B. Not labeling the type of information to be retained

C. Applying the longest retention periods to the information

D. Applying shorter retention periods to the information

Question: 187

Which type of security control does NOT include CCTV cameras?

A. Corrective

B. Deterrent

C. Preventive

D. Detective

Question: 188

A security consultant hired to design the security policies for the PHI within an organization will be primarily handling:

A. Personal Health information

B. Public Health information

C. Procedural Health information

D. Protected Health information

Question: 189

Which of these cloud deployment models is a combination of public and private cloud storage?

A. Community

B. Private

C. Hybrid

D. Public

Question: 190

What is the primary goal of a Change Management Policy?

A. To standardize the creation of the organization's network and computer systems

B. To guarantee that systems are up to date with the latest security patch

C. To standardize the usage of the organization's network and computer systems

D. To guarantee that system changes are performed without negatively affecting business operations

Question: 191

Which of these is NOT a feature of a SIEM (Security Information and Event Management)?

A. Log auditing

B. Log encryption

C. Log consolidation

D. Log retention

Question: 192

Which of these technologies is the LEAST effective means of preventing shared accounts?

A. Requiring a one-time password via an application

B. Requiring one-time passwords via a token

C. Password complexity requirements

D. Requiring biometric authentication

Question: 193

Which of these is NOT a best practice in access management?

A. Trust but verify

B. Periodically assessing whether user permissions still apply

C. Giving only the right amount of permission

D. Requesting a justification when upgrading permission

Question: 194

(★) When analyzing risks, which of these activities is required?

A. Accepting all evaluated risks

B. Identifying risks associated with loss of confidentiality

C. Determining the likelihood of occurrence of a set of risks

D. Selecting the appropriate controls

Question: 195

Which of these exercises goes through a sample of an incident step-by-step, validating what each person will do?

A. A simulation exercise

B. A walk-through exercise

C. A tabletop exercise

D. A checklist exercise

.

Question: 196

(★) Which of these types of documents is usually THE LEAST formal?

A. Standards

B. Guidelines

C. Policies

D. Regulations

Question: 197

A backup that captures the changes made since the latest full backup is an example of:

A. A differential backup

B. An incremental backup

C. A backup snapshot

D. A full backup

Question: 198

A high-level executive of an organization receives a malicious email that tries to trick him. Which attack is the perpetrator using?

A. DDOS

B. Whaling

C. Phishing

D. Spear phishing

Question: 199

What does redundancy mean in the context of cybersecurity?

A. Designing systems with robust components, so that the organization has more attack resilience

B. Conceiving systems with only the most necessary components, so that the organization has just the necessary risks.

C. Conceiving systems with less attack surface, so that the attacker has less chance of success

D. Conceiving systems with duplicate components so that, if a failure occurs, there will be a backup

Question: 200

When a company collects PII, which policy is required?

A. Remote Access Policy

B. GDPR

C. Privacy Policy

D. Acceptable Use Policy

Question: 201

Which type of attack PRIMARILY aims to consume all the available resources, thereby making an organization's service inaccessible to its intended users?

A. Trojans

B. Cross-Site Scripting

C. Denial of Service

D. Phishing

Question: 202

Which one of these tools is MOST likely to detect an XSS vulnerability?

A. Network vulnerability scanner

B. Static application test

C. Intrusion detection system

D. Web application vulnerability scanner

Question: 203

Which kind of physical access control is LESS effective at preventing unauthorized individual access to a data center?

A. Turnstiles

B. Barriers

C. Fences

D. Bollards

Question: 204

Which of these is NOT a type of malware?

A. Trojan

B. Worm

C. Spoofing

D. Rootkit

Question: 205

Which security principle states that a user should only have the necessary permission to execute a task?

A. Privileged Accounts

B. Separation of Duties

C. Least Privilege

D. Defense in Depth