Practice CompTIA+ Exam 1

- Due No due date
- Points 99
- Questions 99
- Time Limit 100 Minutes

Instructions

The actual CompTIA Security+ exam has a maximum of 90 questions with a 90-minute time limit. This practice quiz has 99 questions, so I imposed a 100-minute time limit. Please take the exam as you would the actual exam and follow what you know and your instincts. This practice exam does not count towards the grade in the Foundations of Cybersecurity class. I'm sure there are questions that we haven't covered, just give it your best try.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	68 minutes	88 out of 99

Correct answers are hidden.

Submitted Oct 31 at 12:15pm

IncorrectQuestion 1

0 / 1 pts

Emma is the CEO of a bank. She has received an email that is encouraging her to click on a link and fill out a survey. Being security conscious, she normally does not click on links. However, this email calls her by name and claims to be a follow-up to a recent conference she attended. Which of the following best describes this attack?

○ Vishing

○ Social engineering

● Spear phishing

○ Whaling

Question 2

1 / 1 pts

Isaac has conducted a port scan and identified a service running on TCP port 389. What port would he typically expect the secure version of the same service to run on?

○ 983

○ 389

● 636

○ 836

Question 3

1 / 1 pts

Jerome's company has suffered from a number of security incidents recently due to successful phishing attacks that send users to malicious websites. Jerome wants to prevent access to those sites. Which of the following options will provide him with the ability to do so and to make it easy to block new threats?

● A content or URL filter and a subscription to a filter list service

○ A firewall and regular manual updates based on the most recent phishing attacks

○ DKIM and SPF with regular updates to MX records

○ A DLP and content aware rules

Question 4

1 / 1 pts

The organization that Janet works for is concerned about state actors as a threat model. What type of threats should she prepare to face?

○ Website defacement

○ Phishing attacks

● Advanced persistent threats

○ Ransomware

IncorrectQuestion 5

0 / 1 pts

Which factor is the best indicator of an encryption key's strength once you know the encryption algorithm in use?

○ Whether the key is stretched

● If the key is salted

○ The key length

○ The slope of its elliptic curve

Question 6

1 / 1 pts

Ursula needs to explain the concept of certificate stapling to her organization's web team. Which of the following best describes OCSP stapling?

○

It attaches an X.509 certificate to a cryptographic private key, simplifying the Transport Layer Security (TLS) transaction.

●

It connects a time-stamped OCSP response signed by the CA to the TLS handshake, allowing clients to bypass the need to contact the CA directly.

○

It attaches a symmetric key to an X.509 certificate, allowing clients to use less computationally complex encryption for the remainder of the web session.

○

It connects a time-stamped public key to the private key originally sent by a server, completing the X.509 certificate for the client.

Question 7

1 / 1 pts

What component of a modern PC can act as a random number generator, create cryptographic keys for specific purposes, and help with remote attestation processes for boot-time-loaded drivers and other components?

○ A PKI

● A TPM

○ An HSM

○ An SBUS

Question 8

1 / 1 pts

There is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and privileges than what is required for the tasks the user needs to fulfill. This is the opposite of what principle?

○ Separation of duties

● Least privileges

○ Transitive trust

○ Account management

Question 9

1 / 1 pts

Rae receives an anonymous tip that an attacker intends to perform a watering hole attack against her organization. What target should she seek to monitor and possibly protect?

○ The company's primary file server

○ The organization's food and beverage systems

● The websites most frequently visited by the company's employees

○ The break room PC

Question 10

1 / 1 pts

Kyle wants to ensure that he has an appropriate level of geographic dispersal for his organization's two datacenters. What distance should he place them at?

○ Inside the same town to allow for staff to reach either datacenter in an emergency

○ At a distance where latency will not impact systems communications

● At a distance where a single disaster is unlikely to impact both datacenters

○

At the maximum distance that they can afford to be separated by to minimize the chance of disasters ever impacting both at once

Question 11

1 / 1 pts

Meena is looking for a type of access control that enforces authorization rules by the operating system. Users cannot override authentication or access control policies. Which of the following best fits this description?

○ DAC

● MAC

○ RBAC

○ ABAC

Question 12

1 / 1 pts

Alaina needs to set up a wireless network using WPA2. She wants to support encryption but does not have the ability to use Enterprise authentication mode. What is her best option?

● PSK

○ A captive portal

○ Open Wi-Fi

○ SAE

Question 13

1 / 1 pts

Lilly is responsible for security on web applications for her company. She is checking to see that all applications have robust input validation. What is the best way to implement validation that she can trust?

● Server-side validation

○ Client-side validation

○ Validate in transit

○ None of the above

Question 14

1 / 1 pts

Cynthia wants to bypass port security to gain access to a network. What technique is most likely to help her gain access to the network if port security is enabled?

○ ARP spoofing

○ VLAN hopping

● MAC cloning

○ IP spoofing

Question 15

1 / 1 pts

Jim believes that one of his staff members is attempting to log in as another user on a Windows system. He knows that the user whose credentials were stolen changed their password, but he still wants to find evidence in the logs of the attempted logins. Which Windows log should he check, and what type of event will he be looking for?

○ The security log, and a warning

○ The system log, and a success audit

○ The application log, and a warning

● The security log, and a failure audit

Question 16

1 / 1 pts

Cameron wants to ensure that Voice over IP (VoIP) traffic is prioritized in his network as part of a network security design focused on identifying which traffic is most important. What technology can he use to do this across his entire network?

○ Port security

● QoS

○ ACLs

○ Port taps

Question 17

1 / 1 pts

Henry wants to conduct a risk assessment for his organization and needs to calculate the exposure factor (EF) for a system. What type of assessment should be conducted?

● A quantitative risk assessment

○ A residual risk assessment

○ A functional risk assessment

○ A qualitative risk assessment

IncorrectQuestion 18

0 / 1 pts

Michelle is deploying wireless IoT sensors throughout her organization's facilities and intends to connect them to the network. What common security risk should she be aware of before connecting her IoT devices to the network?

○ Lack of computational power

○ Weak default settings

○ Lack of cryptographic support

● All of the above

Question 19

1 / 1 pts

How is the integrity of forensic artifacts verified?

○ Using cryptographic salts

○ By using full-disk encryption

● By comparing MD5 or SHA1 hashes

○ By using a cryptographic nonce

Question 20

1 / 1 pts

An attacker is trying to get malformed queries sent to the backend database to circumvent the web page's security. What type of attack depends on the attacker entering text into text boxes on a web page that includes special characters and commands that are designed to be inserted into database queries?

● SQL injection

○ Clickjacking

○ Cross-site scripting

○ Bluejacking

Question 21

1 / 1 pts

Hinata is considering biometric access control solutions for her company. She is concerned about the crossover error rate (CER). Which of the following most accurately describes the CER?

○ The rate of false acceptance

○ The rate of false rejection

○ The point at which false rejections outpace false acceptances

● The point at which false rejections and false acceptances are equal

Question 22

1 / 1 pts

Nicole wants to conduct a forensic analysis of a drive that she has imaged. Which of the following tools would be best suited to provide her a timeline of what occurred on the system the drive was imaged from?

● Autopsy

○ dd

○ WinHex

○ FTK Imager

Question 23

1 / 1 pts

Laura wants to prevent users from using their company-issued devices when they are not in corporate facilities. What account policy should she set to ensure this occurs?

○ Geotagging

○ Time-based logins

○ Impossible travel time/risky login

● Geofencing

Question 24

1 / 1 pts

What nonbinding legal document is used to describe how two organizations want to act toward each other or in coordination with each other?

○ An SLA

○ An NDA

● An MOU

○ A BPA

Question 25

1 / 1 pts

Choose the correct order of volatility when collecting digital evidence.

○ Hard disk drive, DVD-R, RAM, swap file

○ Swap file, RAM, DVD-R, hard disk drive

○ RAM, DVD-R, swap file, hard disk drive

● RAM, swap file, hard disk drive, DVD-R

Question 26

1 / 1 pts

Which of the following descriptions best describes a tabletop exercise?

○ An exercise set up to run like a game, allowing responders to score points and compete against one another

●

Staff members who will be involved in a response process discussing a scenario or scenarios in an informal review process

○ Any exercise that is run in a room with a table

○ An exercise that is intended to resemble a real event as closely as possible

Question 27

1 / 1 pts

Tom has been asked to implement a solution that will help his organization apply least privilege principles to local administrative accounts as well as to Windows domain accounts. What type of solution should he look for?

● A PAM solution

○ A DAC solution

○ An SSO solution

○ A CHAP solution

Question 28

1 / 1 pts

Jack wants to set up automated indicator sharing (AIS) through his threat intelligence tool. What standard language should he ensure that his threat feed supports to allow him to pull the threat data into most modern threat tools?

○ Python

○ SAML

● STIX

○ ThreatML

Question 29

1 / 1 pts

Susan logs in at the university she is attending and can then use her credentials to access systems at other universities around the country, because those institutions trust her home institution and give her rights based on her membership and account there. What concept is she taking advantage of?

○ MDM

● Federation

○ OAuth

○ SAE

Question 30

1 / 1 pts

Tracy wants to find evidence of SQL injection attacks against her Apache web server on a Debian server. Which of the following locations is most likely to contain evidence of those attacks?

○ auth.log

● access.log

○ system.log

○ secure.log

Question 31

1 / 1 pts

Jason wants to implement an always-on virtual private network (VPN) for his company. What VPN technology should he use?

● An IPSec VPN

○ An SAML VPN

○ An SSL VPN

○ An SSH VPN

Question 32

1 / 1 pts

Which of the following best describes residual risk?

○ Risk that remains after insurance is purchased is man-made risks

● Risk that remains after controls are implemented for inherent risks

○ Risk that remains due to a lack of patches and updates

○ Risk that remains due to undiscovered vulnerabilities like zero-day exploits

Question 33

1 / 1 pts

A user in Jill's organization has reported that he believes that someone is controlling his machine remotely. What type of malware is Jill most likely to find if this is true?

○ A worm

● A RAT

○ A virus

○ A CROW

IncorrectQuestion 34

0 / 1 pts

Which of the following would prevent a user from installing a program on a company-owned mobile device?

○ Allow lists

● Deny lists

○ ACL

○ HIDS

Question 35

1 / 1 pts

You have instructed all administrators to disable all nonessential ports on servers at their sites. Why are nonessential ports a security issue that you should be concerned about?

● Nonessential ports provide additional areas of attack.

○ Nonessential ports can't be secured.

○ Nonessential ports are less secure.

○ Nonessential ports require more administrative effort to secure.

Question 36

1 / 1 pts

In 2019, VxWorks vulnerabilities were announced that could allow for remote code execution. What is the most severe issue that this type of vulnerability in a real-time operating system (RTOS) results in?

● Attackers could gain remote administrative control of impacted devices.

○ Attackers could crash impacted devices.

○ Attackers could cause a denial-of-service condition for impacted devices.

○ Attackers could gather information from impacted devices.

Question 37

1 / 1 pts

Helen has been asked to review her organization's wireless security and discovers that the organization is using an open Wi-Fi network. What recommendation should Helen make to most significantly increase the security of the network?

○ Implement a captive portal to provide secure access to the network.

○ Implement WPA2 in SAE mode.

● Implement WPA2 Enterprise.

○ Implement WPA2 PSK.

Question 38

1 / 1 pts

Kristen is building a red team for her company and wants to select a tool to help them quickly conduct penetration tests. Which of the following tools will provide them with an automated means of collecting penetration test data?

○ curl

○ Cuckoo

○ PowerShell

● sn1per

Question 39

1 / 1 pts

What is a wildcard certificate used for?

○ Multiple domains

○ Multiple systems from multiple domains

○ Multiple servers with the same name

● Multiple subdomains of a domain

Question 40

1 / 1 pts

What is the primary concern Megan should have about zero-day vulnerabilities that might impact her web server software?

○ They cannot be patched.

○ They cannot be detected by an IPS.

○ They cannot be blocked by a firewall.

● They cannot be acted on until they are disclosed.

Question 41

1 / 1 pts

Charles wants to protect data at rest in his cloud computing environment. What is his best option to ensure that it cannot be stolen?

○ Tokenization

○ Data minimization

● Encryption

○ Hashing

Question 42

1 / 1 pts

Selah wants to quickly add an additional line to a file using a single command at the command line. What command-line tool should she use?

○ netcat

○ head

○ tail

● cat

Question 43

1 / 1 pts

Laurel knows that her organization is in an area where lightning strikes frequently cause power disruptions. She has a generator but also knows that her generator is slow to start, so she wants to add a UPS. What type of control is she adding?

○ A detective control

○ A deterrent control

● A compensating control

○ An operational control

Question 44

1 / 1 pts

John is a salesman for an automobile company. He recently downloaded a program from an unknown website, and now his client files have their file extensions changed and he cannot open them. He has received a pop-up window that states his files are now encrypted and he must pay .5 bitcoins to get them decrypted. What has happened?

○ His machine has a rootkit.

○ His machine has a logic bomb.

○ His machine has a boot sector virus.

● His machine has ransomware.

Question 45

1 / 1 pts

Lucca wants to identify open services on systems throughout his network. What tool can he use to scan for and identify those services?

○ dig

○ hping

○ arp

● nmap

Question 46

1 / 1 pts

Ian's organization has implemented DNSSEC for their Domain Name System (DNS) environment, and Ian needs to explain to his management what it does. Which of the following descriptions accurately describes the security improvement that DNSSEC provides?

○ It provides end-to-end encryption using TLS for DNS queries.

● It cryptographically authenticates DNS data and provides data integrity.

○ It uses symmetric encryption to allow DNS servers to conduct secure zone transfers and updates.

○ All of the above

Question 47

1 / 1 pts

Derek wants to access a filesystem on a machine that has experienced an operating system failure that prevents it from booting. What nonpersistent option will allow him to boot the system without the operating system working?

○ Reverting to a known good state

● A live boot tool

○ A last-known good configuration checkpoint

○ A reinstallation of the operating system

Question 48

1 / 1 pts

Jerome is following the order of volatility and needs to preserve a system's memory state, its disk drive, and backups of the system. Which order should he work from, from most volatile to least volatile?

○ Backups, memory, disk drives

○ Memory, backups, disk drives

○ Disk drive, memory, backups

● Memory, disk drive, backups

Question 49

1 / 1 pts

Which recovery site is the easiest to test?

○ Warm site

○ Cold site

● Hot site

○ Medium site

IncorrectQuestion 50

0 / 1 pts

Mikayla believes that the system she is reviewing may have fallen victim to a DLL injection attack. What type of malware is she most likely to find?

● A RAT

○ Memory-resident malware

○ A worm

○ Spyware

Question 51

1 / 1 pts

Megan's company is preparing to move to a continuous integration/continuous delivery (CI/CD) environment. Which of the following is not a typical component of a continuous delivery pipeline?

● Analysis

○ Continuous deployment

○ Feedback

○ Visibility

Question 52

1 / 1 pts

Tom logs into his Google account to access services on a photo-editing site. What role is Google playing in this scenario?

● An IdP

○ An SP

○ An IDS

○ An DLP

Question 53

1 / 1 pts

Melissa has installed a fire suppression system. What type of strategy is Melissa's company engaging in?

○ Risk acceptance

○ Risk avoidance

○ Risk transference

● Risk mitigation

Question 54

1 / 1 pts

You are the head of the IT department of a school and are looking for a way to promote safe and responsible use of the Internet for students. With the help of the teachers, you develop a document for students to sign that describes methods of accessing the Internet on the school's network. Which of the following best describes this document?

○ Service level agreement

● Acceptable use policy

○ Incident response plan

○ Chain of custody

Question 55

1 / 1 pts

Emily is setting up a load balancer and wants to ensure that systems can connect to it and access resources. What does she need to set up to ensure this?

○ A round-robin NAT

○ A transit gateway

● A VIP

○ An ARP interpreter

Question 56

1 / 1 pts

What is the primary danger of false negatives in vulnerability scans?

○ Vulnerabilities that are not there may be identified.

○ Incorrect patches may be installed.

● Systems may be vulnerable but identified as safe.

○ Services may crash due to the use of the wrong plug-in for testing.

Question 57

1 / 1 pts

Jacinda has a number of Extensible Authentication Protocol (EAP) modes to choose from and is considering EAP-TLS for her wireless network. What requirement of EAP-TLS makes it harder to manage for large installations?

○ Private keys need to be changed on a regular basis, typically less than one year.

● Certificates must be managed for both clients and servers.

○ Each system must be manually updated from EAP-SSL to EAP-TLS.

○ The PAC, or protected access credential, needs to be manually provisioned to each client.

Question 58

1 / 1 pts

Brian is building a data classification scheme for his company. Which of the following classification categories is the least protected and secure?

● Public

○ Private

○ Sensitive

○ Confidential

Question 59

1 / 1 pts

During a conversation with another colleague, you suggest there is a single point of failure in the single load balancer in place for the company's SQL server. You suggest implementing two load balancers in place, with only one in service at a given time. What type of load balancing configuration have you described?

○ Active-active

○ Active Directory

○ Round robin

● Active-passive

Question 60

1 / 1 pts

The company that Gary works for has identified the need to run separate systems for credit card processing and general office use. Unfortunately, the organization does not have space or funds to put secondary systems in place and so instead opts to use dedicated credit card processing devices. What type of control is this?

○ Preventive

○ Managerial

● Compensating

○ Deterrent

Question 61

1 / 1 pts

A user is redirected to a different website when the user requests the Domain Name System (DNS) record www.xyz.com. Which of the following is this an example of?

● DNS poisoning

○ DoS

○ DNS caching

○ Smurf attack

Question 62

1 / 1 pts

Sean wants to help protect his organization's new facility by making it less likely to be targeted by casual attackers who may notice things like corporate signs, logos, or flashy buildings. What technique should he use to help keep his company's new building off attackers' radar?

○ Anonymous building

○ Screened facilities

● Industrial camouflage

○ Corporate armor

Question 63

1 / 1 pts

Paul wants to ensure that the cryptographic system he is using will not expose data even if the session keys originally set up for data exchange are compromised. What feature is he looking for in a cryptosystem?

○ Continuous key obfuscation (CKO)

● Perfect forward secrecy (PFS)

○ Quantum cryptography

○ Ephemeral salting

Question 64

1 / 1 pts

Scott was using his company's wireless network and then noticed he lost connection. Shortly afterward, he was able to reconnect. What type of wireless attack is most likely to have occurred if this was a malicious event?

○ Jamming

● Disassociation

○ Evil twin

○ Wi-snarfing

Question 65

1 / 1 pts

Kathleen wants to implement a touchless payment system for her company. What wireless technology is most frequently used for touchless payment?

○ Bluetooth

○ Infrared

● NFC

○ Wi-Fi

Question 66

1 / 1 pts

Which environment is most frequently used for vulnerability scans in organizations with mature development lifecycles if service outages are a major concern?

○ Development

● Staging

○ Test

○ Production

Question 67

1 / 1 pts

Olivia has implemented UEFI Measured Boot and knows that it will perform an action when it is done. What occurs at the end of a measured boot process?

○ Attestation to the user via the UEFI bootloader screen

○ Attestation to the operating system via an OS plug-in

○ Attestation to the operating system via a native OS tool

● Attestation to a remote attestation server

Question 68

1 / 1 pts

STIX, or Structure Threat Information Expression, uses a standard vocabulary for threat actor sophistication. Which of the following terms best describes the sophistication that you would expect a script kiddie to have as described by a STIX threat feed?

○ Innovator

○ Expert

○ Practitioner

● Novice

Question 69

1 / 1 pts

Ryan has recently signed a legal agreement with a service provider that provides a 10 percent refund of their monthly service fees for a cloud service if an interruption occurs that lasts longer than four hours. What type of legal document has Ryan most likely signed?

○ An MOU

● An SLA

○ An NDA

○ A BPA

Question 70

1 / 1 pts

Mary has noticed that when her organization's applications receive unexpected input they show details of the local directory, SQL code, and other details of what occurred that led to the problem. What concern should she express to the developers in her organization?

- ● A need for better error handling
- ○ A need for regular data backups
- ○ They need to ensure they are using encrypted data transmission.
- ○ They should implement strong authentication.

Question 71

1 / 1 pts

Systems that Nolan's employer has recently purchased have come with malware installed on them. The vendor claims that the systems are leaving their production floor without malware on them. What is the primary risk that Nolan should identify in this scenario?

- ○ Lack of vendor support
- ● Supply chain
- ○ System integration
- ○ Data storage

IncorrectQuestion 72

0 / 1 pts

The company that Chris works for is located in an area that is frequently struck by hurricanes. Which of the following solutions should he implement in his cloud-hosted environment to ensure that a regional disruption of the cloud provider does not cause his website to become unavailable?

- ○ Load balancing
- ○ RAID
- ○ HA across zones
- ● CASB

IncorrectQuestion 73

0 / 1 pts

Joe wants to select an attack framework to help his organization describe adversary tools and tactics in ways that are used across the industry. Which of the following frameworks is the most broadly adopted and integrated with existing tools?

- ○ The Diamond Model of Intrusion Analysis
- ○ MITRE ATT&CK
- ○ The Cyber Kill Chain

● The COOP model

IncorrectQuestion 74

0 / 1 pts

Carlos works in incident response for a midsized bank. Users inform him that internal network connections are fine but that connecting to the outside world is very slow. Carlos reviews logs on the external firewall and discovers tens of thousands of Internet Control Message Protocol (ICMP) packets coming from a wide range of different IP addresses. What type of attack is occurring?

● Smurf

○ DoS

○ DDoS

○ SYN flood

Question 75

1 / 1 pts

You are comparing biometric solutions for your company, and the product you pick must have an appropriate false acceptance rate (FAR). Which of the following best describes FAR?

● How often an unauthorized user is granted access by mistake

○ How readily users accept the new technology, based on ease of use

○ How often an authorized user is not granted access

○ How frequently the system is offline

Question 76

1 / 1 pts

Xyla notices that the gas pump she is using has an added module that reads her credit card as she inserts it. When she pulls on it, it comes off of the pump, revealing additional hardware inside that looks like a cellular modem and a camera. What type of attack has she likely uncovered?

● Skimming

○ A malicious USB attack

○ A card cloning attack

○ A brute-force attack

Question 77

1 / 1 pts

What administrative control should Ujama implement to reduce the likelihood of malicious actions by new hires in his organization?

○ Install a camera system that monitors their work.

● Conduct background checks for all new employees.

○ Install locks on all the doors that new employees should not enter or access.

○ Use automated theft detection software to identify patterns of behavior that may be malicious.

Question 78

1 / 1 pts

Alyssa is setting up the mobile device management tool her company recently bought and wants to ensure that staff members who are issued a mobile device do not use unapproved applications. Which of the following can give her the complete control of applications that can be installed?

● An application approved list

○ An application deny list

○ A go/no-go list

○ None of the above

Question 79

1 / 1 pts

What does the term "known environment test" mean?

● The tester has full knowledge of the environment.

○ The tester works with the environment daily and has helped construct it.

○ The tester has permission to access the system.

○ The tester has no permission to access the system.

Question 80

1 / 1 pts

Emma wants to calculate the mean time between failures for a device in her organization. How should she calculate the MTBF?

○ The annual rate of occurrence multiplied by the expected useful lifetime of the device

○ The average number of failures per day divided by the number of days the company is open per year

○ The number of failures that have occurred in one year divided by 365

● The total number of operational hours divided by the number of failures during that time period

IncorrectQuestion 81

0 / 1 pts

Jared wants to generate, store, and manage cryptographic keys on a mobile device for his organization. What solution would be best suited to this purpose?

● A mobile TPM

○ A microSD HSM

○ An embedded cryptoprocessor

○ A MDM

Question 82

1 / 1 pts

As part of a penetration test process, Michelle and Tony want to determine what wireless networks are accessible in a multiblock area where a large hospital and affiliated offices operate. What technique should they use to find as many wireless networks as possible as quickly as possible?

○ War chalking

○ Vulnerability scanning

○ Wi-sniping

● War driving

Question 83

1 / 1 pts

Theresa is doing application testing and runs a tool that sends random and unexpected inputs to the application to see how it responds. What type of testing is she doing?

○ Unit testing

● Fuzzing

○ Static code analysis

○ Fagan testing

Question 84

1 / 1 pts

Mike is a network backup engineer and performs a full backup each Sunday evening and an incremental backup Monday through Friday evenings. One of the company's network servers crashed on Thursday afternoon. How many backups will Mike need to do to restore the server?

○ Two

○ Three

● Four

○ Five

Question 85

1 / 1 pts

Chris is attempting to social engineer his way into an organization and tells the staff member that he is targeting that they will be responsible for the company not getting a major contract if they do not assist him. What social engineering principle is he using?

○ Authority

● Intimidation

○ Consensus

○ Familiarity

Question 86

1 / 1 pts

What common datacenter design technique orients machines to all pull air from one side and exhaust it out the other as part of temperature management in the facility?

● Hot aisle/cold aisle

○ Passive datacenter heating

○ Active datacenter cooling

○ An air gap

Question 87

1 / 1 pts

Which of the following outlines a business goal for system restoration and allowable data loss?

● RPO

○ Single point of failure

○ MTTR

○ MTBF

IncorrectQuestion 88

0 / 1 pts

Emiliano is considering voice recognition as part of his access control strategy. What is one weakness with voice recognition?

● People's voices change

○ Systems require training

○ High false negative rate

○ High false positive rate

Question 89

1 / 1 pts

When systems in Amanda's organization query the Domain Name System (DNS) server for domains related to malware and other suspect activities, the DNS server responds with incorrect information, pointing the systems to a harmless IP address. What type of security solution has Amanda's organization implemented?

○ A DNS round-robin

○ A DNS tarpit

● A DNS sinkhole

○ None of the above

Question 90

1 / 1 pts

What type of attack is it when the attacker attempts to get the victim's communication to abandon a high-quality/secure mode in favor of a lower-quality/less secure mode?

● Downgrade

○ Brute force

○ Rainbow table

○ Bluesnarfing

Question 91

1 / 1 pts

When Rick tests his company's web application, he discovers that some tests seem to behave differently based on timing. In fact, when it receives two queries at the same time, it does not consistently provide the same result. Sometimes, it gives a correct answer, and at other times the queries result in the wrong response. What type of issue has Rick most likely discovered?

○ A SQL injection flaw

○ A fuzzer response

● A race condition

○ A replay attack

Question 92

1 / 1 pts

Joanna's manager has told her that she needs to prevent sideloading of applications to the organization's mobile devices. What methods should she focus on preventing?

○ Loading of files via USB

○ Loading of files via memory card

○ Loading of files via wireless

● All of the above

Question 93

1 / 1 pts

A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?

○ Token

● Multifactor

○ Kerberos

○ Biometrics

IncorrectQuestion 94

0 / 1 pts

You are attending a meeting with your manager and he wants to validate the cost of a warm site versus a cold site. Which of the following reasons best justify the cost of a warm site?

● The company is likely to lose only a small amount of income during long downtime.

○ The company may lose a large amount of income during short downtime.

○ A warm site will cost more than a hot site but will allow faster restoration.

○ A cold site allows faster restoration but will cost more.

Question 95

1 / 1 pts

Jason wants to implement self-encrypting drives for his organization with full-disk encryption used to keep data secure at rest. What standard should he ensure that the drives support?

○ STONE

○ RUBY

○ ROCK

● OPAL

Question 96

1 / 1 pts

What computing concept is closely associated with fog computing?

○ Container-based architectures

● Edge computing

○ Thin clients

○ Service-oriented architectures

Question 97

1 / 1 pts

Frank has discovered a wireless network broadcasting the same SSID that his network provides, but when he connects to it, it is not one of his company's access points. What type of attack has he discovered?

○ A SSID clone attack

○ A mirrored AP

● An evil twin

○ An evil maid

Question 98

1 / 1 pts

Which of the following is not a type of log that will be captured using journald, and thus made available via journalctl?

○ initrd logs

○ Kernel logs

● Web server logs

○ Service logs

Question 99

1 / 1 pts

What common network security tool is the best equivalent to a security group in cloud service environments?

● A firewall

○ An intrusion detection system (IDS)

○ An intrusion prevention system (IPS)

○ Security information and event management (SIEM)