# CompTIA CASP+ - Quiz Questions with Answers

## 1.0 Security Architecture



**1.**

A software development company wants to test its code in an environment where it cannot make changes to the operating system or other files outside of its restricted area. Which type of solution should they use for this?

- **Sandboxing**
- Code signing
- Jailbreaking
- Clustering

*Correct answer: Sandboxing*

*Sandboxing is a technique for limiting the ability of code to affect the rest of the system. This can be useful for testing an application in development or for running untrusted applications.*

*Code signing is used to verify an application's author and that the code has not changed in transit. Jailbreaking is the process of removing restrictions imposed by a device's manufacturer or provider. Clustering is used for improved performance and fault tolerance.*

**2.**

What term describes residual data that remains on storage media after deletion?

- **Data remanence**
- Watermarked data
- Protected enclaves
- Memory leak data

---

*Correct answer: Data remanence*

*Data remanence is residual data that remains on storage media after deletion. In many cases, simply deleting data does not completely remove it from a storage media. Ensuring data remanence is addressed is an important part of avoiding data leakage.*

*Watermarking is a digital rights management technique that indicates data ownership. For example, a watermark on a photo may indicate the marketing agency that owns it.*

*Protected enclaves is an approach to data zone creation that focuses on implementing controls based on the importance and sensitivity of the data in a given area.*

*A memory leak occurs when programs do not properly release unused memory allocations.*

**3.**

A small-sized company of a few people will start hiring more employees soon. Currently, each user manages their own workstation, and each user takes a different approach to making sure their computer is secure. What should the company implement in order to ensure that each user has a baseline of security for their system?

**Policies**

Availability zones

NAC lists

FIM

---

*Correct answer: Policies*

*Policies are used to enforce a standard operating system environment. In Windows, Group Policy is used with Active Directory to administer settings.*

*Availability zones are independent locations within a region when using cloud computing. A Network Access Control (NAC) list is a list of rules that define who can access a resource. File Integrity Monitoring (FIM) is used to keep track of changes to important files.*

**4.**

Of the following, which type of chip makes full-drive encryption possible?

- **TPM**
- Out-of-band
- ASLR
- TLS

---

*Correct answer: TPM*

*Full-disk encryption implementations, like Windows BitLocker, often require a Trusted Platform Module (TPM). The TPM is a chip located in the motherboard that can store and use password protection, digital rights management, and enables full-disk encryption. The TPM chip houses the keys used to encrypt a system drive and decrypt it upon startup. This can protect against the hard drive being removed and inserted into another system to attempt to exfiltrate data.*

*TLS is a common form of encryption for data in transit, but not a type of chip. Out-of-band is a form of access that does not use a standard network, such as dial-in or cellular access to an Ethernet LAN. Address space layout randomization (ASLR) is a technique that helps prevent attacks that attempt to corrupt memory.*

**5.**

Which of the following is NOT an access authentication protocol?

**DNSSEC**

LDAP

CHAP

PAP

---

*Correct answer: DNSSEC*

*LDAP, CHAP, PAP, and MS-CHAP v2 are all examples of an access authentication protocol. DNSSEC is not an access authentication protocol. DNSSEC uses digital signatures to validate the authenticity of DNS servers.*

**6.**

What data sensitivity label should be applied to PHI?

**High impact**

Unrestricted

Moderate impact

Public

---

*Correct answer: High impact*

*PHI (protected health information) is subject to HIPAA regulations in the U.S. and could cause severe negative impact if leaked. Using NIST data sensivity labels, PHI should be labeled "high impact."*

*PHI data disclosure would generally be considered greater than moderate impact and PHI should not be labeled unrestricted or public.*

**7.**

A company wants to enable integration by using middleware to move messages between unlike services. What type of solution should they adopt for this?

**ESB**

SOA

DNS

LDAP

---

*Correct answer: ESB*

*The Enterprise Service Bus (ESB) is the middleware that handles the communication between software applications in an SOA. Different providers of ESB provide products with varying functionalities.*

*Service-Oriented Architecture (SOA) is an approach to building modular, reusable, and interoperable services. DNS is used to translate domain names to IP addresses. LDAP (Lightweight Directory Access Protocol) is a directory service.*

**8.**

Which of the following decouples the network hardware layer from the network control layer?

- **SDN**
- MPLS
- VLAN
- VPC

---

*Correct answer: SDN*

*SDN (software-defined networking) is the virtualization of network technologies that creates a software-defined control plane that is decoupled from hardware. Virtualizing the control plane enables more flexibility and control in network management.*

*MPLS (multiprotocol label switching) is a network protocol used to connect multiple network locations.*

*A VLAN (virtual local area network) is a logically isolated network segment.*

*A VPC (virtual private cloud) is a logically isolated environment in a public cloud.*

**9.**

Which of the following options is a benefit of a network design that places a VPN appliance in a screened subnet on the network firewall?

**It enables inspection of decrypted VPN traffic**

It is highly scalable

It eliminates the need for a DNS server

It enables DNSSEC

---

*Correct answer: It enables inspection of decrypted VPN traffic*

*There are multiple options for VPN placement in a network. The different options include:*

- *VPN in parallel with the firewall*
- *VPN inside a screened subnet*
- *An integrated VPN and firewall appliance*

*A key benefit of running a VPN in a screened subnet on a network firewall is that the firewall can inspect decrypted VPN traffic. A tradeoff of this approach is it may lead to limitations on bandwidth scalability.*

*Running a VPN in a screened subnet does not directly impact the need for or use of a DNS server or DNSSEC.*

**10.**

IPsec is a suite of  protocols. Of the following IPsec protocols, which handles the creation of a security association for the session and key exchange?

**ISAKMP**

IKE

ESP

AH

---

*Correct answer: ISAKMP*

*Internet Security Association and Key Management Protocol (ISAKMP) handles the creation of the security association for the session and key exchange.*

*Authentication Header (AH) provides data integrity, data origin authentication, and protection from replay attacks.*

*Encapsulating security payload (ESP) provides all that AH does plus data confidentiality.*

*Internet Key Exchange (IKE) is also sometimes referred to as IPsec key exchange. IKE provides the authentication material used to create the keys exchanged by ISAKMP during peer authentication. This was proposed to be performed by a protocol called Oakley that relied on the Diffie-Hellman algorithm, but Oakley was superseded by IKE.*

**11.**

Of the following, which is NOT a safe computer operating practice?

**Enabling autorun for USB drives**

Performing daily security scans

Not clicking suspicious email links

Keeping anti-malware applications current

---

*Correct answer: Enabling autorun for USB drives*

*Disabling autorun for USB drives is a common vector-oriented security control. Enabling autorun increases exposure to vulnerability risks from USB drives infected with malware.*

*Daily security scans, not clicking suspicious email links, and keeping anti-malware applications updated are all good security practices.*

**12.**

What is the minimum number of drives that RAID 0 and RAID 1 need to operate?

- **2**
- 3
- 4
- 1

*Correct answer: 2*

*RAID 0 and RAID 1 require a minimum of 2 drives.*

**13.**

Which of these threats can DNSSEC help prevent?

**DNS cache poisoning**

Sniffing DNS traffic

DDoS attacks against a DNS server

DNS amplification attacks

---

*Correct answer: DNS cache poisoning*

*DNSSEC is a protocol that helps prevent man-in-the-middle attacks against DNS by using digital signatures to sign DNS responses. With DNSSEC, you can limit the risk of attacks like DNS cache poisoning and DNS hijacking.*

*DNSSEC does not encrypt the actual DNS traffic. Traffic can still be sniffed even if DNSSEC is implemented. DNSSEC does not prevent denial of service (DoS) attacks. DDoS and DNS amplification attacks are types of DoS attacks.*

**14.**

Which of the following is NOT a standard type of HTTP header?

**Post**

Request

Response

Entity

---

*Correct answer: Post*

*Post is a type of HTTP request, not an HTTP header type.*

*Request, response, and entity are all standard HTTP header types.*

**15.**

Which type of solution addresses the threat of data exfiltration?

- **DLP**
- Microsegmentation
- ACL
- SNMP trap

---

*Correct answer: DLP*

*Data Loss Prevention (DLP) is a solution to prevent the exfiltration of data. It can be installed on end-point systems or at the edges of a network to stop the transfer of sensitive data.*

*Microsegmentation is used to improve security and efficiency by dividing networks into smaller segments. An Access Control List (ACL) is used for controlling access to a resource. An SNMP (Simple Network Management Protocol) trap is used for sending information to an SNMP manager.*

**16.**

Of the following, which is a nonprofit foundation that maintains a list of the top 10 web application security risks?

**OWASP**

CompTIA

RFC

ISO

---

*Correct answer: OWASP*

*The Open Web Application Security Project (OWASP) is a nonprofit foundation that aims to improve software security. OWASP maintains a list of top 10 attacks against web apps known as the OWASP Top Ten. OWASP holds regular meetings at chapters throughout the world and provides resources and tools, including testing procedures and development guidelines.*

*CompTIA is the trade association that offers a variety of certifications, including the CASP+.*

*ISO (International Organization for Standardization) creates a variety of standards for technical fields.*

*RFC (request for comments) is a type of standards document.*

**17.**

What advantage does homomorphic encryption have for security?

**It allows computations to be performed on encrypted data without decrypting it.**

It enables a continuously growing list of records that are linked and secured cryptographically.

It uses superposition and entanglement to perform computations related to encryption.

It makes predictions and decisions based on training data without being explicitly programmed to do so.

---

*Correct answer: It allows computations to be performed on encrypted data without decrypting it.*

*Homomorphic encryption allows computations on encrypted data without decrypting it. This is useful because it enhances the privacy of the data.*

*Blockchain enables a continuously growing list of records that are linked and secured cryptographically. Quantum computing uses superposition and entanglement to perform computations. Machine learning makes predictions and decisions based on training data without being explicitly programmed to do so.*

**18.**

Alice, a security analyst at Acme Inc., recently installed a hardware appliance that monitors network activity and restricts connectivity for devices that do not meet certain network security requirements.

What type of solution is this?

**Hardware-based NAC**

FIM

Software-based VPNs

SIEM

---

*Correct answer: Hardware-based NAC*

*Hardware-based NAC uses a physical network appliance to monitor and control network access. If non-compliant devices are detected, a hardware based NAC can restrict connectivity.*

*FIM (file integrity monitoring) monitors files for changes and can send an alert when a file is modified.*

*Software-based VPNs are used to create secure private networks over public networks like the Internet.*

*A security information and event management (SIEM) tool aggregates and analyzes logs and other security event information. SIEMs are useful tools for identifying suspicious network activity and determining when and how an attacker may have breached a network.*

**19.**

A company wants to improve its security by hardening user authentication. They would like to add an ownership factor to authentication that is based on something a user has. Which of the following factors will meet this requirement?

**Token device**

Password

Signature dynamics

Finger scan

---

*Correct answer: Token device*

*Using multiple factors of authentication can improve user identification. Token devices are physical devices issued to a user, so they are ownership factors that a user has.*

*A password is a knowledge factor that a person knows. Signature dynamics is an action factor that is something a person does. A finger scan is a characteristic factor that is something a person is.*

## 20.

The increased usage of cloud computing, remote work, and mobile devices has altered how organizations approach security. Which security model have organizations adopted to handle this unique threat?

**Zero trust**

RBAC

IAM

Perimeter security

---

*Correct answer: Zero trust*

*In the modern computing environment, there are no clear perimeters due to ever-changing network topologies. A zero-trust model is used, which considers even internal devices as untrusted by default.*

*Role-Based Access Control (RBAC) assigns permissions based on responsibilities in an organization. Identity and Access Management (IAM) focuses on managing user identities and access rights. Perimeter security focuses on external threats.*

**21.**

Which of the following is a type of data flow enforcement?

- **ACL**
- SSH
- SMTP
- HTTPS

*Correct answer: ACL*

*An ACL (access control list) is a type of data flow enforcement in that it can restrict or allow access based on criteria like source, destination, and network port.*

*SSH, SMTP, and HTTPS are all network communication protocols.*

## 22.

Attacks that make use of improperly configured prompts to the user, such as SQL injection, can be solved with what technique?

**Input validation**

Entry sanitation

Secure session management

PKI

---

*Correct answer: Input validation*

*Input validation can solve issues that arise from web applications that do not validate the data entered by the user (or a hacker). Input validation is the process of checking all input for things such as proper format and proper length. In many cases, these validators use either the blocklisting of characters or patterns or an allow list of characters or patterns.*

*"Entry sanitation" is not a standard cybersecurity term. Secure session management does not directly relate to user input and is a generic term for securely handling how user sessions are created, maintained, and ended. Public key infrastructure (PKI) is a system for managing digital certificates.*

**23.**

What is the purpose of requiring that mobile apps be signed?

**To ensure the authenticity and integrity of an app**

To allow for the app to be sideloaded

To make sure that the app is compatible with multiple devices

To show that the app has been tested and is free of bugs

---

*Correct answer: To ensure the authenticity and integrity of an app*

*Code signing is used to verify the authenticity and integrity of a mobile app. If an unsigned app is installed on a device, the device should be assumed to be untrusted.*

*Sideloading involves installing an app from a location other than the device's main app store. Compatibility and bug testing are related to app development.*

**24.**

A company is looking to improve the resiliency of its website. They already have a cluster of load-balanced servers. They now want to build in logic that can help the cluster better react to changes in the environment in real time. What type of solution should they implement?

**Course of action orchestration**

Distributed allocation

Runbooks

Steganalysis

---

*Correct answer: Course of action orchestration*

*Course of action orchestration is used to automate entire workflows. It can be used to address changing workflows.*

*Distributed allocation refers to locating critical assets in different locations. Runbooks are step-by-step instructions for IT teams to follow during incidents. Steganalysis is the process of finding hidden information in digital media.*

**25.**

Bob, a security engineer at Acme Inc., configures an IDS threshold that compares this week's network traffic to last week's and alerts if the difference is too high. What type of IDS threshold is this?

**Historical**

State-based

Fixed

Static

---

*Correct answer: Historical*

*Historical thresholds consider past and present values and are often used to compare different periods. An IDS threshold that compares one week's traffic to a previous week is an example of a historical threshold.*

*Alert thresholds based on fixed numeric values or calculations are called fixed thresholds. A 95% CPU utilization threshold is an example of a fixed value.*

*State-based thresholds are triggered when a system state changes, such as a server beginning a graceful shutdown or starting up after rebooting.*

*Static is not a standard type of IDS threshold.*

**26.**

Which of the following is a system that receives information from logs and centralizes this data for analysis?

**SIEM**

INE

HSM

IDS

---

*Correct answer: SIEM*

*Security information and event management (SIEM) utilities receive information from log files of critical systems and centralize the collection and analysis of this data. SIEM technology is an intersection of two closely related technologies: security information management (SIM) and security event management (SEM).*

*An inline network encryptor (INE), also called a high-assurance internet protocol encryptor (HAIPE), is a type 1 encryption device. Type 1 designation indicates that it is a system certified by the NSA for use in securing US government classified documents. To achieve this designation, the system must use NSA-approved algorithms.*

*A hardware security module (HSM) is an appliance that safeguards and manages digital keys used with strong authentication and provides crypto processing. It attaches directly to a computer or server.*

*An intrusion detection system (IDS) is a cybersecurity tool that helps detect potentially malicious behavior. There are a couple of intrusion-based technologies. An anomaly-based IDS watches the network for a period of time to establish a baseline of operation. After this point, it monitors the network and can determine when things change, such as with a suspected network breach, and alert administrators. Signature-based IDS systems analyze network traffic and match it to known attack patterns. This is similar to antivirus detection, where the system maintains a database of known attacks and what they look like and, thus, can detect them when they appear on the network. This is called pattern matching. The other type is stateful matching, which monitors the operating system state and recognizes any changes that violate the specifically defined rules.*

## 27.

Of the following, which is a benefit of OTA updates?

**Enables remote firmware updates**

Enables local software updates

Allows users to update devices from their docking stations

Prevents devices from booting with unauthorized code

---

*Correct answer: Enables remote firmware updates*

*OTA (over-the-air) updates allow teams responsible for applying updates to software or firmware to apply them remotely without requiring physical access to the devices.*

*OTA updates do not:*

- *Perform local (non-networked) software updates*
- *Directly prevent devices from booting with unauthorized code*
- *Directly allow users to update devices from their docking stations*

**28.**

Which of the following threats is an air-gapped system MOST vulnerable to?

**An insider threat**

Malware from a malicious public file sharing site

Cryptojacking by a compromised Internet-based video streaming platform

DDoS by a botnet

---

*Correct answer: An insider threat*

*Air-gapped systems are not connected to the Internet. Therefore, attacks that depend on Internet access (like malware on the Internet or cryptominers embedded in a streaming platform that uses the Internet) are unlikely to impact an air-gapped system. Similarly, botnets generally carry out DDoS attacks against Internet-facing resources.*

*An insider could potentially compromise an air-gapped system because they can gain access to it without the Internet.*

**29.**

Which of the following is NOT a form of obfuscation?

**Anonymization**

Encryption

Tokenization

Masking

---

*Correct answer: Anonymization*

*Obfuscation refers to a set of techniques that make data difficult to understand or use. Encryption, tokenization, and masking are all examples of obfuscation.*

*Anonymization is a way to remove sensitive personal data from a data set so it can be analyzed and consumed without the personal data.*

**30.**

What type of attack involves the data written to a temporary storage area exceeding the storage area's limit?

**Buffer overflow**

XSS

CSRF

DNSSEC bypass

---

*Correct answer: Buffer overflow*

*A buffer is a type of temporary storage area on a system. A buffer overflow occurs when the data written to a buffer exceeds its limit. Buffer overflows can cause applications to crash or enable a threat actor to execute code.*

*XSS (cross-site scripting) is a type of injection attack commonly used against websites.*

*DNSSEC is a protocol for using digital signatures to authenticate DNS servers. DNSSEC bypass is not a standard name for an attack type.*

*Cross-Site Request Forgery (CSRF) attacks, a.k.a. one-click attacks, aim to get users to perform an unintended action on a web application, usually by clicking a malicious link while they are logged into the app.*

**31.**

Of the following, which does NOT describe a SAN?

**Typically on the same local area network (LAN) as other network devices**

Is easily scalable with ability to add additional storage

Maintenance can be performed without taking servers offline

Provides block-level access to data

---

*Correct answer: Typically on the same local area network (LAN) as other network devices*

*A SAN (storage area network) is generally a dedicated network used to access specific storage devices. A SAN is not typically on the same LAN as other network devices.*

*These points about SANs are all true:*

- *SANs are easily scalable with ability to add additional storage*
- *SANs are able to have maintenance performed without taking servers offline*
- *SANs provide block-level access to data*

**32.**

A company has started turning to more cloud services for its operations. In order to ensure that they still have compliance, threat protection, and data loss prevention when using cloud services, they would like to implement middleware. What type of solution acts as middleware between the end-user organization and its cloud services?

**CASB**

VDI

VPN

SaaS

---

*Correct answer: CASB*

*A Cloud Access Security Broker (CASB) acts as middleware between an end-user organization and cloud services. Examples include Microsoft Cloud App and Cisco Cloudlock.*

*Virtual Desktop Infrastructure (VDI) is used to manage users' virtual desktops on centralized servers. A Virtual Private Network (VPN) is an encrypted tunnel between two endpoints. Software as a Service (SaaS) is used to provide a software package in the cloud.*

**33.**

Which of the following firewall types is aware of all the proper functioning of the TCP handshake, keeps track of the current status of all connections, and can recognize erroneous packets trying to enter the network?

**Stateful inspection firewall**

Packet-filtering firewall

Circuit-level proxy firewall

Application-level proxy firewall

---

*Correct answer: Stateful inspection firewall*

*Firewalls can be discussed on the basis of their type and their architecture. When we discuss different types, we're discussing how they operate differently from one another.*

- *Stateful firewalls - These firewalls are aware of the proper functioning of the TCP handshake, keep track of the state of all connections with respect to this process, and can recognize erroneous packets trying to enter the network.*
- *Packet-filtering firewalls - These firewalls are the least detrimental to throughput as they only inspect the header of the packet for allowed IP addresses or port numbers. While performing this function slows traffic, it involves only looking at the beginning of the packet and making a quick decision.*
- *Proxy firewalls - This type of firewall actually stands between an internal-to-external connection and makes the connection on behalf of the endpoints.*
  - *Circuit-level proxies operate at the session layer (Layer 5) of the OSI model. This type of proxy makes decisions based on the protocol header and session layer information.*
  - *Application-level proxies perform a type of deep packet inspection (up to Layer 7). This type of firewall understands the details of the communication process at Layer 7 for the application.*
- *Dynamic packet filtering - Although this isn't actually a type of firewall, dynamic packet filtering is a process that a firewall may or may not handle and deserves a mention.*
- *Kernel proxy firewalls - This type of firewall is an example of a fifth-generation firewall. It inspects a packet at every layer of the OSI model but does not introduce the same performance hit as an application-layer firewall because it does this at the kernel layer.*

**34.**

Which of the following is a document that details security requirements and supporting documentation?

- **SRTM**
- SAST
- DAST
- CDN

---

*Correct answer: SRTM*

*An SRTM (security requirements traceability matrix) is a document that contains security requirements and supporting documentation. It includes details such as requirement numbers, descriptions, and how to validate the requirements.*

*SAST (static application security testing) tooling scans source code for vulnerabilities, while DAST (dynamic application security testing) tooling checks an application for vulnerabilities at runtime.*

*A CDN (content delivery network) is a network of servers that provides content like images, videos, and web pages to help improve website speed and availability.*

**35.**

Of the following remote control solutions, which is proprietary to Microsoft and can control the remote host as if you were logged into it?

**RDP**

SSH

Telnet

VPN

---

*Correct answer: RDP*

*The Remote Desktop Protocol (RDP) is a proprietary Microsoft technology that enables administrators to remotely control their Microsoft systems as if they were sitting in front of them, unlike telnet and SSH, which only provide command line functionality. RDP sessions use built-in RDP encryption but do not authenticate the session host server. To mitigate this, you can use SSL for server authentication and encrypting session host server communications.*

*VPN (virtual private network) refers to a private network—often implemented via secure tunnels—that runs over an insecure "public" network.*

**36.**

A software development company wants to take a development approach that is incremental and iterative. They want to produce a prototype and do a risk analysis at each stage. What developmental approach should they take?

**Spiral**

Waterfall

SecDevOps

Agile

---

*Correct answer: Spiral*

*The spiral model has each phase start with a design goal and end with a client review. It can be good for large projects, but it is slower than some other models.*

*The Waterfall method does not return to previous stages after they are completed. The SecDevOps approach incorporates security into each phase. The Agile method focuses on continuous feedback.*

**37.**

At times, applications may use the actual name or key of an element when generating a web page. Applications don't always verify that a user is authorized for the target. What type of vulnerability does this result in?

**Insecure direct object reference**

Direct reference insecurity

Application specific allocation

Direct link bypassing

---

*Correct answer: Insecure direct object reference*

*An insecure direct object reference (IDOR) vulnerability occurs when a web application attempts to access an object directly by the name or key of the object without any additional access controls. The attack can come from an authorized user, meaning that the user has permission to use the application but is accessing information to which they should not have access. To prevent this problem, each direct object reference should undergo an access check. Code review of the application with this specific issue in mind is also recommended.*

*Direct reference insecurity, application specific allocation, and direct link bypassing are incorrect answers.*

**38.**

What term describes information about data like EXIF information in a .jpeg file?

**Metadata**

Superdata

XOR data

CMDB data

---

*Correct answer: Metadata*

*Metadata is information about data. EXIF information in a .jpeg file is one example of metadata. Another example is email headers.*

*A CMDB (configuration management database) includes all the CI and relationships between the CI in a given environment.*

*Superdata and XOR data are distractor answers.*

**39.**

Which of the following options is a benefit of a network design that places a VPN appliance in parallel with a firewall appliance?

**It is highly scalable**

It provides centralized content inspection

It is energy efficient

It eliminates the need for a DNS server

---

*Correct answer: It is highly scalable*

*There are multiple options for VPN placement in a network. The different options include:*

- *VPN in parallel with the firewall*
- *VPN inside a screened subnet*
- *An integrated VPN and firewall appliance*

*A key benefit of running a VPN in parallel with a firewall is scalability. With this design, you can use multiple VPN appliances in parallel with your firewall. A tradeoff with this approach is that there is no central content inspection point.*

*This design approach is not necessarily energy efficient and does not eliminate the need for a DNS server.*

**40.**

A company wants to implement APIs to better connect with consumers. All of the following are security issues they should be aware of when managing these APIs EXCEPT:

**Response formats**

Authentication

Authorization

Data scoping

---

*Correct answer: Rate limits*

*Using APIs to let clients can open up vulnerabilities. However, response formats, such as JSON or XML, are not related to security.*

*APIs (Application Programming Interfaces) use authentication to make sure that only allowed parties can connect. APIs use authorization to allow certain resources to authenticate users. APIs use data scoping to ensure that too much data isn't exposed.*

**41.**

Which of the following configurations for a WiFi network is the MOST secure?

**WPA3 with MAC filtering**

WEP with MAC filtering

WEP without MAC filtering

WPA3 without MAC filtering

---

*Correct answer: WPA3 with MAC filtering*

*WPA in general is more secure than WEP for wireless security. MAC filtering adds additional security to wireless networks by only allowing a predetermined set of devices to connect to a network. Therefore, WPA3 with MAC filtering is the most secure WiFi implementation of the four options.*

**42.**

Which of the following is NOT a standard type of software testing?

**Pipeline testing**

Unit testing

User acceptance testing

Regression testing

---

*Correct answer: Pipeline testing*

*Pipeline testing is not a standard type of software testing.*

*Unit testing is the testing of individual blocks ("units") of code during development.*

*User acceptance testing is software testing performed by users to confirm the software meets their needs.*

*Regression testing is a form of testing that occurs after changes to confirm software still works as expected.*

**43.**

What advantage does PAT have for a network?

**To enable devices with private IP addresses to connect to the internet**

To allow different software applications to interact with each other

To detect and prevent attacks against a network

To protect web application servers from various types of attacks

---

*Correct answer: To enable devices with private IP addresses to connect to the internet*

*Port Address Translation (PAT) is a one-to-many mapping of Network Address Translation (NAT) that allows one device to represent an entire private network. This saves on IPv4 addresses, which is useful because IPv4 does not have as large an address space as IPv6.*

*An API (Application Programming Interface) allows different software applications to interact with each other. An IPS (Intrusion Prevention System) detects and prevents attacks against a network. A WAF (Web Application Firewall) is used to protect web application servers from various types of attacks.*

**44.**

Of the following, which was introduced to solve the issues of a previously insecure wireless security method and utilizes the Temporal Key Integrity Protocol for encryption?

**WPA**

RC4

WEP

PSK

---

*Correct answer: WPA*

*WPA was introduced to address security issues with WEP. WPA uses the Temporal Key Integrity Protocol (TKIP) for encryption.*

*WEP was the first security measure used with 802.11 wireless networks. A problem with WEP is how it implements the RC4 encryption algorithm.*

*PSK stands for pre-shared key, which could be used with WEP.*

**45.**

Of the following, which is a group that creates cybersecurity related documentation, methods, and tools for web applications?

**OWASP**

SCAP

ISO

IEC

---

*Correct answer: OWASP*

*The Open Web Application Security Project (OWASP) is a group that monitors attacks, specifically web attacks. They seek to provide additional information to those affected by any cyber attacks and maintain a list of the top 10 attacks impacting web applications (the "OWASP Top 10).*

*The Security Content Automation Protocol (SCAP) is maintained by the National Institute of Standards (NIST) and includes specifications that help standardize cybersecurity automation tasks including vulnerability and compliance management.*

*The International Electrotechnical Commission (IEC) maintains electronic and electrical engineering standards.*

*The International Organization for Standardization (ISO) maintains a variety of engineering standards, but not electronic and electrical engineering standards (which are maintained by the IEC).*

**46.**

What does the iptables command below do?

iptables -A INPUT -s 192.0.2.11 -j DROP

**Block all inbound traffic from IP address 192.0.2.11**

Allow all outbound traffic to 192.0.2.11

Allow all inbound traffic from IP address 192.0.2.11

Update iptables to use the last rules for interface eth1

---

*Correct answer: Block all inbound traffic from IP address 192.0.2.11*

*iptables is a popular open-source firewall used on many Linux systems. CASP+ candidates should be familiar with configuring iptables on Linux systems. The command in the question appends (the A parameter) a rule for input (inbound) traffic from 192.0.2.11 that blocks (DROPs) traffic. It does not specify an interface or allow traffic.*

**47.**

What type of security solution is an "all-in-one" tool that bundles multiple security functions into a single appliance?

**UTM**

RADIUS

NAT

VPN

---

*Correct answer: UTM*

*A UTM (Unified Threat Management) appliance rolls functions like firewalling, antivirus, IPS/IDS, and anti-spyware into a single solution.*

*RADIUS is an open standard for centralizing authentication, authorization, and accounting (AAA).*

*NAT (network address translation) is a networking technique that helps devices with private IPv4 addresses connect to the Internet.*

*VPN (virtual private network) is a solution that enables the creation of a secure private network over another "insecure" network like the public Internet.*

**48.**

Which of the following provisions certificates to devices contained on a network, including mobile devices?

**SCEP**

OTA

Sideloading

Application wrapping

---

*Correct answer: SCEP*

*SCEP (simple certificate enrollment protocol) is used by devices to obtain digital certificates. CERT VU#971035 calls out authentication issues that make SCEP risky outside of closed environments.*

*OTA (over-the-air) is taken from the term "OTA updates." OTA updates allow teams responsible for applying updates to software or firmware to apply them remotely without requiring physical access to the devices.*

*Application wrapping is the process of building a management layer to help implement control over an app without directly modifying it.*

*Sideloading is the process of installing an app from an unauthorized or unofficial source.*

**49.**

What default UDP ports does SNMP (simple network management protocol) use?

**161 and 162**

80 and 443

25, 456, and 587

20 and 21

---

*Correct answer: 161 and 162*

*SNMP (simple network management protocol) uses UDP ports 161 and 162 by default. Port 161 is used for queries (e.g., SNMP GET requests) from an SNMP manager to an SNMP agent. Port 162 is used for messages (e.g., SNMP TRAP messages) from an SNMP agent to an SNMP manager.*

**50.**

What type of services are used to provide organizational information such as users, servers, printers, other resources on a network?

**Directory**

Federation

Peering

STARTTLS

---

*Correct answer: Directory*

*Directory services are used to provide organizational information such as users, servers, printers, other resources on a network. LDAP is an example of a directory service protocol.*

*A federation is a group of domains with an established trust.*

*Peering is a technique for directly connecting two networks.*

*STARTTLS is a command that initiates the use of encrypted network communications.*

**51.**

Which of the following functions is an Application Delivery Controller (ADC) PRIMARILY used for?

**Load balancing traffic across multiple servers**

Translating IP addresses to domain names

Authenticating users in a Windows-based environment

Encrypting end-to-end connection for remote access

---

*Correct answer: Load balancing traffic across multiple servers*

*An ADC has many functions for optimizing the delivery and performance of applications. One feature is load balancing, which distributes traffic across multiple servers to provide fault tolerance and prevent overloading of a single server.*

*A DNS server translates IP addresses to domain names. A domain controller is for authenticating users in a Windows-based environment. A VPN encrypts end-to-end connections for remote access.*

**52.**

Of the following, which is NOT a command-line utility?

**RDP**

ping

netstat

nslookup

*Correct answer: RDP*

*Microsoft's Remote Desktop Protocol (RDP) is used in their Remote Desktop program on Windows systems. The other commands, ping, netstat, and nslookup, all operate within the command prompt on the appropriate operating systems. Combined with switches and input information, they are used through a console, while the RDP protocol is used with a graphical user interface (GUI).*

**53.**

Which of the following is NOT a benefit of VLANs?

**Physical network isolation**

Reduced network congestion

Smaller broadcast domains

Logical network isolation

---

*Correct answer: Physical network isolation*

*Virtual local area networks (VLANs) separate networks by logically isolating them. VLANs are implemented by network devices like managed switches and do not provide physical isolation. Devices connected to the same physical switch could be on different VLANs.*

*By logically isolating networks, VLANs also reduce network congestion and create smaller broadcast domains than a network that includes all connected devices.*

**54.**

What are the transport protocols and default port numbers for DNS?

**TCP and UDP: Port 53**

TCP: Port 53

TCP and UDP: Port 22

TCP: Port 80

---

*Correct answer: TCP and UDP: Port 53*

*As a CASP candidate, it is very important that you know the port numbers of both secure and insecure services and applications. In cases where you need to block or allow a traffic type, you need to know the port number of the traffic type. DNS queries are transmitted using UDP port 53 by default. DNS zone transfers use TCP port 53 by default.*

**55.**

You are a security consultant working for Acme, Inc. The CISO asks you to draft a document that ensures employees handle personal data in a way that is compliant with General Data Protection Regulation (GDPR).

What type of document will meet this requirement?

- **Regulatory policy**
- Advisory policy
- Access control list
- Access log

---

*Correct answer: Regulatory policy*

*A regulatory policy is a policy based on a law or regulatory standards. A policy that aligns internal processes with GDPR is an example of a regulatory policy.*

*Advisory policies explain the consequencies of not performing certain actions or not following specific guidelines. An acceptable use policy is a textbook example of an advisory policy.*

*An access control list (ACL) is a set of rules that limit access to resources. A common example of an ACL is a set of firewall rules that limit access based on network address ranges.*

*An access log is a log file that contains information on who accessed a system and what requests were made.*

**56.**

What term does CompTIA now use instead of DMZ (demilitarized zone) to describe a network segment that provides isolation between untrusted and trusted networks?

**Screened subnet**

VLAN

Class A subnet

Class C subnet

---

*Correct answer: Screened subnet*

*CompTIA has replaced the term DMZ with perimeter network or screened subnet. Perimeter networks provide isolation by defining network perimeters that provide isolation between trusted and untrusted networks.*

*VLANs provide virtual Layer 3 network isolation and can be used to help create perimeter networks, but VLANs are a more general networking concept.*

*Class A and Class C networks are types of classful networks used in IPv4 addressing.*

**57.**

A company is considering options for their data classification, labeling, and tagging. They want to implement a standard for an attribute-based access control system that is decoupled from the application or local machine. Which solution will help with this?

**XACML**

XSS

XSLT

XUL

---

*Correct answer: XACML*

*The eXtensible Access Control Markup Language (XACML) is an XML-based language for access control policies. It can be used to exchange access control policies between different systems.*

*XSS (Cross-Site Scripting) is a type of web security exploit. XSLT (Extensible Stylesheet Language Transformations) is a language for transforming XML (Extensible Markup Language) documents into other formats. XUL is a user interface language.*

**58.**

Which of the following tools can scan plaintext source code for vulnerabilities?

**SAST**

DAST

ITSEC

MPLS

---

*Correct answer: SAST*

*SAST (static application security testing) tooling scans source code for vulnerabilities, while DAST (dynamic application security testing) tooling checks an application for vulnerabilities at runtime.*

*ITSEC (Information Technology Security Evaluation Criteria) is an older standard for validating trusted operating systems.*

*MPLS (multiprotocol label switching) is a network protocol used to connect multiple network locations.*

**59.**

What category of virus techniques target Microsoft Office products like Excel?

**Macro viruses**

Boot record infectors

Program infectors

Multipartite infectors

---

*Correct answer: Macro viruses*

*Computer viruses are constantly evolving and exploit techniques come in a variety of different forms. Some of the most common types of virus techniques include:*

- *Macro viruses - target Microsoft Office products. Enabling macros is often required for these exploits to succeed.*
- *Boot record infectors - target boot records*
- *Program infectors - target executable files (e.g., .exe files and other binaries)*
- *Multipartite infectors - target multiple attack surfaces*

## 60.

A company wants to implement a solution to credentials management that has a low up-front development cost. They decide they will use a system that is portable and can be used across systems controlled by different identities. What type of solution should they implement?

**Federation**

IAM

SSO

MFA

---

*Correct answer: Federation*

*A federation identity system is used for users to access resources across multiple domains. Each member of the federation agrees to a common set of policies and standards.*

*Identity and Access Management (IAM) systems are centralized authentication systems. Single Sign-On (SSO) does not share credentials between systems. Multi-Factor Authentication (MFA) is a way to secure authentication by requiring more than one authentication technique.*

## 61.

As a security architect at Acme, Inc., you need to design a solution that will enable secure data access between multiple non-federated networks. Some of the networks are owned and operated by Acme, Inc. and others are owned and operated by partners.

Which of the following solutions is the BEST option to meet this requirement?

**Cross domain solution**

Virtual private cloud

VLAN

Peering

---

*Correct answer: Cross domain solution*

*A cross domain solution (CDS) enables secure data access across different networks with different security policies. A CDS can consist of both hardware and software and acts as an interface for enforcing policies to allow or deny data transfer.*

*A VPC (virtual private cloud) is a logically isolated environment in a public cloud. A VLAN (virtual local area network) is a logically isolated network segment.*

*Peering is a technique for directly connecting two networks. There are multiple types of peering including:*

- *Public peering - Uses a single Ethernet switch port*
- *Private peering - Uses network-layer hardware to create a point-to-point connection between multiple networks*
- *Paid peering - One party pays another to peer*

## 62.

Which of the following terms describes an environment where new software, upgrades, and patches can be tested in an environment comparable to production prior to a production deployment?

**Staging**

Guest

VPC

Availability zone

---

*Correct answer: Staging*

*A staging environment is a production-like environment that allows organizations to test new software, upgrades, and patches before deploying them to production.*

*A guest environment is an environment used to enable guests (individuals who are not employees, contractors, etc.) to connect and use network resources.*

*A VPC (virtual private cloud) is a logically isolated environment in a public cloud.*

*An availability zone is a geographical datacenter location. Deploying workloads in multiple availability zones helps mitigate single points of failure.*

**63.**

SMTP uses multiple default ports depending on whether or not mail is encrypted and the encryption techniques used. Which of the following is NOT a default SMTP port?

**645**

25

587

465

---

*Correct answer: 645*

*The default port for SMTP (simple mail transfer protocol) is 25. Versions of SNMP that use SSL/TLS use ports 587 and 465 by default. 645 is not a default SMTP port.*

**64.**

Which of the following is a popular host firewall on Linux systems?

**iptables**

NIDS

LDAP

John the Ripper

---

*Correct answer: iptables*

*iptables is a popular open-source firewall used on many Linux systems. CASP+ candidates should be familiar with configuring iptables on Linux systems.*

*A NIDS (network intrusion detection system)is used to monitor and analyze network traffic for potential threats.*

*LDAP is an authentication protocol used for accessing directory services.*

*John the Ripper is a password cracker.*

## 65.

A data analysis company wants to set up a way for external organizations to efficiently and securely retrieve data from them. This system should define how clients will ask for the information and how the response will be made. What type of solution will allow for this?

**API gateway**

SPAN port

Network tap

SNMP trap

---

*Correct answer: API gateway*

*An Application Programming Interface (API) handles interactions between different types of systems. An API gateway can be used to manage API calls from external sources and retrieve and deliver the responses from the application.*

*A Switched Port Analyzer (SPAN) port is a mirrored port. A network tap is a hardware device used for monitoring traffic. A Simple Network Management Protocol (SNMP) trap is a notification message sent from a network device.*

## 66.

What type of rule action tells an intrusion detection system (IDS) to block a and log the activity?

**Drop**

Reject

Sdrop

Logdrop

---

*Correct answer: Drop*

*Intrusion detection systems support a variety of rule actions that allow administrators to define what the system should do with a packet that meets the criteria of a specific rule. Three different ways a rule action can block transmission of a packet are:*

- *Drop- Blocks transmission of a network packet and logs the activity.*
- *Reject- Blocks transmission of a network packet and logs the activity. Sends a TCP reset for TCP traffic. Sends an ICMP unreachable message for UDP traffic.*
- *Sdrop- Blocks transmission of a network packet and does not log the activity.*

*Logdrop is not a standard IDS rule.*

## 67.

Acme, Inc.'s current network design uses a single appliance to integrate VPN and firewall functionality. This design has created a single point of failure Acme, Inc. wants to eliminate. You've been asked to recommend a solution that eliminates the single point of failure.

Which of the following options is the BEST choice?

**A mirrored VPN and firewall**

A centralized SIEM

An LDAP server that supports X.500 directory services

Endpoint-based NAC

---

*Correct answer: A mirrored VPN and firewall*

*Network designs that integrate VPN and firewall functionality create potential single points of failure. If the firewall fails, the VPN may also fail and vice versa. Mirroring your VPN and firewall helps mitigate this risk.*

*A SIEM aggregates and analyzes security and log information in a central location. It does not eliminate single points of failure.*

*LDAP is an access and authentication protocol. It does not directly address the problem of eliminating single points of failure for VPN and firewall services.*

*Endpoint-based NAC (network access control) uses agents installed on network endpoints and a central management console to enforce network access policies.*

**68.**

Bob, a security engineer at Acme Inc., configures a threshold to send an alert when a firewall's CPU exceeds 95% utilization. What type of threshold is this?

**Fixed**

State-based

Historical

Fatigued

---

*Correct answer: Fixed*

*Alert thresholds based on fixed numeric values or calculations are called fixed thresholds. A 95% CPU utilization threshold is an example of a fixed value.*

*State-based thresholds are triggered when a system state changes, such as a server beginning a graceful shutdown or starting up after rebooting.*

*Historical thresholds consider past and present values and are often used to compare different periods.*

*Fatigued is a distractor answer based on the term "alert fatigue." Alert fatigue can occur if thresholds are not properly configured and users are sent too many notifications causing them to overlook the events that are most important.*

**69.**

An application developer needs to implement software that will work with disparate systems. They would rather focus on the core aspects of their system rather than the details of how to communicate with different operating systems. What type of software will help them with this?

**Middleware**

Container

API

Sandbox

---

*Correct answer: Middleware*

*Middleware is the software between an application and an operating system. They often use messaging frameworks like SOAP (Simple Object Access Protocol), REST (Representational State Transfer), and JSON (JavaScript Object Notation) to provide messaging services for applications.*

*Containers are applications with all their dependencies in a single package. APIs (Application Programming Interfaces) are rules and protocols for two systems to interact with each other. A sandbox is a protected area where an application can be run so that it cannot affect the rest of the system.*

**70.**

Which of the following commands could you use to view open ports, connections, and traffic statistics on a server?

- **netstat**
- df
- nslookup
- nfdump

---

*Correct answer: netstat*

*The netstat ("network statistics") command is a popular command-line tool for displaying information such as open ports, network interface statistics, connections, and routing tables.*

*The nfdump command can be used to extract network flow information for a particular flow or conversation. The nslookup command is used to lookup information related to DNS records. The df ("disk free") command is used to view disk space statistics on Linux systems.*

**71.**

All of the following are examples of network segmentation EXCEPT:

**Network taps**

VLANs

Air gaps

Screened subnets

---

*Correct answer: Network taps*

*A network tap copies all traffic on a network for monitoring purposes. It does not divide a network into smaller networks.*

*VLANs create segmented virtual networks that are created by switches. Air gaps create networks that are physically isolated. Screened subnets, or DMZs, are segmented by firewalls.*

**72.**

POP3 (Post Office Protocol) uses different default ports for clear text and encrypted traffic. What are the two default POP3 port numbers?

**110 for clear text traffic and 995 for encrypted traffic**

25 for clear text traffic and 587 for encrypted traffic

143 for clear text traffic and 993 for encrypted traffic

80 for clear text traffic and 433 for encrypted traffic

---

*Correct answer: 110 for clear text traffic and 995 for encrypted traffic*

*By default, the POP3 (Post Office Protocol) uses port 110 for clear text traffic and 995 for encrypted traffic. Both TCP and UDP ports are registered, but POP3 implementations generally use TCP.*

**73.**

Which of the following is NOT one of the categories that make up the OWASP Top 10 Application Security Risks for 2021?

**Buffer overflow**

Insecure design

Injection

Server-side request forgery

---

*Correct answer: Buffer overflow*

*Injection (#3), insecure design (#4), and server-side request forgery (#10) are all categories in the OWASP Top 10 Application Security Risks for 2021.*

*While a buffer overflow may result from an exploit in one or more of the categories, buffer overflow is not one of the ten categories.*

**74.**

Which of the options below allows devices with private IPv4 addresses to connect to the Internet while also preventing direct connections from the Internet to those devices?

**NAT gateway**

IPS

IDS

STARTTLS

---

*Correct answer: NAT gateway*

*A NAT (network address translation) gateway allows devices with private IPv4 addresses to connect to the Internet while also preventing direct connections from the Internet to those devices.*

*IPS (intrusion prevention system) and IDS (intrusion detection systems) analyze system and network behavior to detect, and, in the case of IPS, prevent potential threats.*

*STARTTLS is a form of opportunistic TLS used to encrypt email traffic.*

**75.**

Which of these systems is LEAST vulnerable to zero-day threats that originate on the Internet?

**An air-gapped system**

A public P2P file sharing system

A system behind a NAT gateway

A system that uses a signature-based antivirus

---

*Correct answer: An air-gapped system*

*An air-gapped system is not connected to the Internet at all. Therefore, it is not directly exposed to Internet-borne threats.*

*A public P2P (peer-to-peer) file sharing system is likely to have some exposure to the Internet.*

*A system behind a NAT (network address translation) gateway is not directly connected to the Internet, but can still reach the Internet via the gateway. This makes a system behind a NAT more vulnerable than an air-gapped system when it comes to Internet-borne threats.*

*A signature-based antivirus does not offer protection against zero-day threats because the attack signature of the threat is not yet known.*

**76.**

IPsec is a suite of  protocols. Of the following protocols, which provides data confidentiality?

- **ESP**
- AH
- ISAKMP
- IKE

---

*Correct answer: ESP*

*Encapsulating security payload (ESP) provides data confidentiality.*

*Authentication Header (AH) provides data integrity and authentication. Internet Security Association and Key Management Protocol (ISAKMP) handles the creation of the security association for the session and exchange keys. Internet Key Exchange (IKE) is also sometimes referred to as IPsec Key Exchange. It provides the authentication material used to create the keys exchanged by ISAKMP during peer authentication.*

## 77.

A software development company has created many new features to an application that they publish. They want to automatically test that old features have not been broken by the additional updates. What type of testing should they implement?

**Regression testing**

Unit testing

Validation testing

Acceptance testing

---

*Correct answer: Regression testing*

*Regression testing is done to make sure that bugs were not introduced after making new changes. New features can often introduce bugs to previous functionality.*

*Unit testing is when individual units of code are tested to ensure they work as intended. Validation testing is done to ensure that the application meets delivery requirements. Acceptance testing is used to make sure that an application meets end user expectations.*

**78.**

An auditor is looking at the secure design patterns that an application developer uses. They find that the application: was designed with security in mind first, rather than as an afterthought; has a configuration setting that makes it secure after being configured correctly after installation; and gives security recommendations about the environments it will be installed into. Given this information, what should the auditor recommend?

**Make the application secure by default.**

Make the application secure by design.

Make the application secure by deployment.

Don't make any changes to the application.

---

*Correct answer: Make the application secure by default.*

*An application needs to be secure by design, default, and deployment. If the application needs configuration changes to be secure after installation, then it is not secure by default.*

*An application is secure by design if security is the top priority during development. An application is secure by deployment if the environment it is introduced to is secure.*

**79.**

An enterprise needs to implement virtualization to improve the availability of its servers. They require that the solution be as efficient as possible by running directly off the hardware without an intermediary operating system. What type of solution should they implement?

**Type 1 hypervisor**

Type 2 hypervisor

VMware Workstation

VirtualBox

---

*Correct answer: Type 1 hypervisor*

*A Type 1 hypervisor has the hypervisor running directly on the hardware. This type is also referred to as a native or bare metal hypervisor and examples include Citrix XenServer, Microsoft Hyper-V, and VMware vSphere.*

*A Type 2 hypervisor runs off a host operating system. VMware Workstation and VirtualBox are examples of Type 2 hypervisors.*

**80.**

Which of the following is NOT a benefit of a UTM appliance?

**Avoids single points of failure**

Streamlines administration

Condenses multiple security functions into one appliance

Provides firewalling and IPS/IDS functions

---

*Correct answer: Avoids single points of failure*

*Because UTM (Unified Threat Management) appliances roll multiple security functions such as firewalling, IPS/IDS, VPN functionality, and antimalware into a single appliance, they also inherently create a single point of failure.*

*A key benefit of UTM is streamlining security administration and management by consolidating multiple appliances into one.*

**81.**

What types of computer viruses change their signature when they replicate?

**Polymorphic viruses**

Macro viruses

Program infectors

Boot record infectors

---

*Correct answer: Polymorphic viruses*

*Polymorphic viruses change their signature when they replicate. By changing their signature, polymorphic viruses make it harder for signature-based antivirus to detect them.*

*Macro viruses target Microsoft Office programs like Excel.*

*Program infectors are a type of virus that target executable files.*

*Boot record infectors are a type of virus that target boot records.*

## 82.

Alice, a wireless engineer at Acme Inc., wants to restrict what devices can connect to a Wi-Fi network without requiring passwords. What solution below is the BEST fit for the requirements?

**Use MAC filtering**

Implement 802.11b Wi-Fi

Use WPA2

Use WPA3

---

*Correct answer: Use MAC filtering*

*MAC filtering allows devices to connect to a wireless network based on their MAC address and does not require a password to authenticate.*

*802.11b is an older Wi-Fi standard that would not directly address the use case of restricting Wi-Fi access without using passwords.*

*Wi-Fi protected access (WPA) implementations like WPA2 and WPA3 require passwords.*

**83.**

Which of the statements below about signature-based and heuristic-based antivirus programs is FALSE?

**Signature-based antivirus is better at detecting polymorphic viruses**

Heuristic-based antivirus is better at detecting zero-day threats

Heuristic-based antivirus often uses AI

Signature-based antivirus needs regular updates

---

*Correct answer: Signature-based antivirus is better at detecting polymorphic viruses*

*Heuristic-based antivirus detects threats based on behavior patterns. This makes heuristic-based antivirus better at detecting zero-day and polymorphic threats that do not have a known signature. Heuristic-based antivirus often uses AI to detect malicious behavior.*

*Signature-based antivirus uses program signatures to detect threats, making it useful for detecting and containing known threats. Because new viruses emerge regularly, signature-based antivirus require regular updates to ensure they have the latest signatures.*

**84.**

A company wants to allow its users to access informational resources by a unique name within the organization's namespace, rather than IP or MAC addresses. Which type of service can they use to accomplish this?

**LDAP**

DHCP

SDN

NAC

---

*Correct answer: LDAP*

*The Lightweight Directory Access Protocol (LDAP) is a directory service protocol for making resources available to users. It uses an object data format where each object has attributes and is referenced by a unique name.*

*DHCP (Dynamic Host Configuration Protocol) is used to assign IP addresses. SDN (Software-Defined Perimeter) is used for managing a network centrally. NAC (Network Access Control) is used for controlling which devices can connect to a network.*

**85.**

All networks evolve, grow, and change over time. Of the following guidelines, which should NOT be part of a change management process?

**Once approved, the change steps should be immediately deployed**

All changes should be formally requested

Each request should be analyzed to ensure that it supports all goals and policies

All changes should be documented

---

*Correct answer: Once approved, the change steps should be immediately deployed*

*Formal change management processes should ensure testing occurs before changes are deployed.*

*Change management processes generally begin with a formal request. If approved, the request then goes through a planned review where the change is analyzed and tested. If those steps pass, a scheduled rollout occurs. All changes should be documented and teams should have a roll back plan in the event a change fails to work as planned.*

## 86.

Management has requested a solution that will connect an in-house Java application with another internally developed .NET solution in order to provide a front end to sales that incorporates the data into a cohesive front end.

Of the following, which solution would you recommend?

**ESB**

CRM

GRC

SOA

---

*Correct answer: ESB*

*An ESB (enterprise service bus) is a type of middleware abstraction layer that is used to enable communication between different services in an SOA (service-oriented architecture).*

*A CRM (customer relationship management) system is used to store information related to sales, marketing, and customer support activities.*

*GRC refers to governance, risk, and compliance, which is one of the main topics of the CASP+ exam.*

**87.**

What secure methodology includes steps like conducting code reviews focused on security and building security into development?

- **Security by design**
- Security by default
- Security by obscurity
- Security by baseline

---

*Correct answer: Security by design*

*Security by design refers to building security into the development of a system and includes steps like secure software development and code reviews that aim to identify security problems.*

*Security by default refers to secure default settings enforced on a system.*

*Security by obscurity refers to security that is not cryptographically secure, but depends on making information harder to find (e.g., changing a default port number). Security by obscurity alone is not a recommended security practice.*

*Security by baseline is a distractor answer.*

## 88.

Before deploying changes to a production server, Acme, Inc. first deploys them to a replica of the production server and evaluates performance for a week. What term BEST describes the replica of the production server?

**Staging environment**

Guest environment

VPC

VPN

---

*Correct answer: Staging environment*

*Staging environments are non-production environments that closely mirror production and are used for testing changes prior to deployment. Staging environments can help teams validate that changes will not negatively impact production.*

*A guest environment is an isolated environment where non-employees can connect to perform specific tasks (e.g., a guest WiFi network). Isolating the guest environment from environments with sensitive data or critical resources helps reduce risk.*

*A VPC (virtual private cloud) is a logically isolated private cloud that runs on shared public cloud infrastructure.*

*A VPN (virtual private network) creates secure (encrypted) private networks over insecure public networks like the Internet.*

**89.**

A company has two remote offices. The CEO wants the networks on each to be connected as if they were local to each other. What type of solution should they implement for this?

**Site-to-site VPN**

Remote access VPN

NAC

NAT

---

*Correct answer: Site-to-site VPN*

*A site-to-site VPN is used to connect two remote networks. It provides a secure and encrypted connection over an untrusted network.*

*A remote access VPN is used to create an encrypted tunnel between one remote user and an internal network. Network Access Control (NAC) is used to authenticate devices before allowing them on a network. Network Address Translation (NAT) is used to give access to the internet to systems with internal IP addresses.*

**90.**

Of the following RAID types, which provides the fastest speeds and offers no data redundancy?

- **RAID 0**
- RAID 1
- RAID 5
- RAID 3

---

*Correct answer: RAID 0*

*RAID 0 combines disks and writes data across them simultaneously with a technique called data striping. It is faster than the other RAID types listed, but if a single disk fails with RAID 0, data is lost.*

*RAID 1, 3, and 5 all offer some form of data redundancy.*

**91.**

Management approaches you about suggested solutions for tracking the state of assets, such as products, systems, software, facilities, and people. They're also deeply interested in the relationships between these assets, as they believe it will help fine-tune IT spending and resources.

Which solution do you recommend?

**CMDB**

SPIT

DNS

Active Directory

---

*Correct answer: CMDB*

*A configuration management database (CMDB) keeps track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets. The IT department typically uses CMDBs as data warehouses.*

*DNS and Active Directory are directory services implementations that enable resource lookup based on names.*

*SPIT (spam over Internet telephony) is a spam technique that targets VoIP.*

**92.**

A company is looking to outsource the development of its marketing website. Which document is a legal agreement that defines the MINIMUM performance criteria for the company that will provide the web development service?

**SLA**

MoU

RFP

SoW

*Correct answer: SLA*

*A Service Level Agreement (SLA) is used to outline the minimum requirements of a service provider. It will also outline any penalties should these services not be met.*

*A Memorandum of Understanding (MoU) is an agreement made before a legal contract is made. A Request for Proposals (RFP) is a document asking vendors to submit proposals to complete a specified job. A Statement of Work (SoW) is a document with a detailed description of a job that has to be done.*

**93.**

Of the following, which allows a user to remove some of the controlling mechanisms that restrict user access and control over a mobile device?

**Rooting**

TPM

MPLS

Push notification

---

*Correct answer: Rooting*

*Rooting a device allows a user to have a deeper level of control over it, because it bypasses the security mechanisms meant to protect items such as the boot image or the primary operating system image from any non-vendor sources. This is called "jailbreaking" in iOS and "rooting" in the Android community.*

*A trusted platform module (TPM) is a type of secure processor.*

*MPLS (multiprotocol label switching) is a network protocol used to connect multiple network locations.*

*Push notification services send messages on a mobile phone even when the application is not open and running on the device. Developers should not place confidential data or intellectual property in a push message.*

**94.**

A company wants an easy way to deploy more server instances for its website. Their solution should allow for their web application to be easily started up along with all its dependencies while using the least amount of resources as possible. What type of solution will enable this?

**Containerization**

Type 2 virtualization

CDN

Caching

---

*Correct answer: Containerization*

*Containerization is the bundling of an application along with its dependencies. This allows the application to be portable as well as only being shipped with the dependencies it requires.*

*Type 2 virtualization is a type of virtualization that runs on top of a host operating system rather than directly on hardware. A Content Delivery Network (CDN) is a geographically dispersed network that serves content based on a user's location. Caching is used to store frequently accessed information.*

**95.**

Which of the following is a protocol that devices can use to obtain digital certificates?

**SCEP**

VNC

VPC

OTA

---

*Correct answer: SCEP*

*SCEP (simple certificate enrollment protocol) is used by devices to obtain digital certificates. CERT VU#971035 calls out authentication issues that make SCEP risky outside of closed environments.*

*VNC (virtual network computing) is a way to enable remote access and access device interfaces remotely.*

*VPC (virtual private cloud) is a logically isolated environment in a public cloud.*

*OTA (over-the-air) is taken from the term "OTA updates." OTA updates allow teams responsible for applying updates to software or firmware to apply them remotely without requiring physical access to the devices.*

**96.**

Which of the following is NOT a zero trust principle?

**Only trust users that have access to secure networks**

Have a single source of truth for user identity information

Do not trust any user or system by default

Implement strong user authentication

---

*Correct answer: Only trust users that have access to secure networks*

*The zero trust security model is based on a philosophy of no trust by default, regardless of the source network or user making a request. Only trusting users that have access to secure networks is an example of older "castle-and-moat" style security that is not consistent with zero trust principles.*

*Having a single source of truth for user identity information, not trusting any user or system by default, and implementing strong user authentication are all legitimate zero trust principles.*

**97.**

A software developer is having an issue with their code not performing the business logic correctly. They want to test the application by going through each line of code line by line without the application running. What type of application should they perform?

**SAST**

DAST

IAST

Fuzz testing

---

*Correct answer: SAST*

*Static Application Security Testing (SAST) is a manual form of testing. The application is not running and the developer goes through it line by line or with the help of an automated tool.*

*Dynamic Application Security Testing (DAST) involves having the application running while code review tools are used. Interactive Application Security Testing (IAST) combines DAST and SAST. Fuzz testing involves sending unexpected data to see how it reacts.*

**98.**

All of the following are core components of a mobile device's hardware root of trust EXCEPT:

**Data minimization**

Device integrity

Isolation

Protected storage

---

*Correct answer: Data minimization*

*A hardware root of trust is needed to provide the foundation of trustworthiness for a device. Data minimization refers to the practice of only collecting the minimal amount of data to perform a function.*

*Device integrity is the security for hardware, firmware, and software. Isolation protects against unintended interactions between applications. Protected storage preserves the confidentiality and integrity of data on the device.*

**99.**

Biometric security, key card access, and locking server racks are all examples of which of the following security controls?

**Physical**

Logical

Technical

Administrative

---

*Correct answer: Physical*

*In contrast to logical controls, which prevent access at the system level, physical access pertains to the presence of one's access to the hardware or location itself. Items such as biometric locks, key card access panels, and locked server racks all prevent access to the device at a physical level.*

*Logical controls—also known as technical controls—are security controls which limit access to systems at a virtual level, like username/password based authentication and authorization, firewall rules, and encryption.*

*Administrative controls include the business processes, procedures, and policies that an organization implements to protect systems.*

## 100.

As a security engineer at Acme Inc., you've been tasked with implementing a solution that will detect when an unidentified device connects to your wireless network. Which of the tools below offers the BEST solution?

**WIDS**

HIDS

WAF

SSH

---

*Correct answer: WIDS*

*A WIDS is like an NIDS for wireless networks. A WIDS (wireless intrusion detection system) can detect and alert when an unidentified wireless device connects to a wireless network.*

*A HIDS (host intrusion detection system is used to monitor and analyze endpoint activity for potential threats. A WAF (web application firewall) is a security tool for protecting against a variety of layer 7 attacks. SSH is an encrypted network communications protocol.*