A6. A company has hired a third-party to gather information about the company's servers and data. This third-party will not have direct access to the company's internal network, but they can gather information from any other source. Which of the following would BEST describe this approach?

- ❍ **A.** Vulnerability scanning
- ❍ **B.** Passive reconnaissance
- ❍ **C.** Supply chain analysis
- ❍ **D.** Regulatory audit

.....

The Answer: B. Passive reconnaissance
Passive reconnaissance focuses on gathering as much information from open sources such as social media, corporate websites, and business organizations.

The incorrect answers:
A. Vulnerability scanning
Some active reconnaissance tests will query systems directly to see if a vulnerability currently exists.

C. Supply chain analysis
A supply chain analysis will examine the security associated with a supplier, and the analysis will not provide any information regarding a company's own servers and data.

D. Regulatory audit
A regulatory audit is a detailed security analysis based on existing laws or private guidelines. A regulatory audit commonly requires access to internal systems and data.

More information:
SY0-701, Objective 5.5 - Penetration Tests
https://professormesser.link/701050502

A7. A company's email server has received an email from a third-party, but the origination server does not match the list of authorized devices. Which of the following would determine the disposition of this message?

- ❍ **A.** SPF
- ❍ **B.** NAC
- ❍ **C.** DMARC
- ❍ **D.** DKIM

The Answer: C. DMARC
DMARC (Domain-based Message Authentication Reporting and Conformance) specifies the disposition of spam emails. The legitimate owner of the originating email domain can choose to have these messages accepted, sent to a spam folder, or rejected.

The incorrect answers:
A. SPF
SPF (Sender Policy Framework) is a list of all authorized mail servers for a specific domain. All legitimate emails would be sent from one of the servers listed in the SPF configuration.

B. NAC
NAC (Network Access Control) is a way to limit network access to only authorized users. NAC is not commonly used to manage the transfer of email messages.

D. DKIM
DKIM (Domain Keys Identified Mail) provides a way to validate all digitally signed messages from a specific email server. DKIM does not determine how the receiving server categorizes these digitally signed messages.

More information:
SY0-701, Objective 4.5 - Email Security
https://professormesser.link/701040505

A8. Which of these threat actors would be MOST likely to attack systems for direct financial gain?

- ❍ **A.** Organized crime
- ❍ **B.** Hacktivist
- ❍ **C.** Nation state
- ❍ **D.** Shadow IT

The Answer: A. Organized crime
An organized crime actor is motivated by money, and their hacking objectives are usually based around objectives that can be easily exchanged for financial capital.

The incorrect answers:
B. Hacktivist
A hacktivist is focused on a political agenda and not commonly on a financial gain.

C. Nation state
Nation states are already well funded, and their primary objective is not usually based on revenue or income.

D. Shadow IT
Shadow IT describes part of the organization that works around the existing IT department to build their own applications and infrastructure.

More information:
SY0-701, Objective 2.1 - Threat Actors
https://professormesser.link/701020101

A9. A security administrator has examined a server recently compromised by an attacker, and has determined the system was exploited due to a known operating system vulnerability. Which of the following would BEST describe this finding?

- ❍ **A.** Root cause analysis
- ❍ **B.** E-discovery
- ❍ **C.** Risk appetite
- ❍ **D.** Data subject

.....

The Answer: A. Root cause analysis
The goal of a root cause analysis is to explain the ultimate cause of an incident. Once the cause is known, it becomes easier to protect against similar attacks in the future.

The incorrect answers:
B. E-discovery
E-discovery relates to the collection, preparation, review, interpretation, and production of electronic documents. E-discovery itself is not involved with the research and determination of an attack's root cause.

C. Risk appetite
A risk appetite describes the amount of risk an organization is willing to take before taking any action to reduce that risk. Risk appetite is not part of a root cause analysis.

D. Data subject
A data subject describes any information relating to an identified or identifiable natural person, especially when describing or managing private information about the subject.

More information:
SY0-701, Objective 4.8 - Incident Planning
https://professormesser.link/701040802

A10. A city is building an ambulance service network for emergency medical dispatching. Which of the following should have the highest priority?

- ❍ **A.** Integration costs
- ❍ **B.** Patch availability
- ❍ **C.** System availability
- ❍ **D.** Power usage

The Answer: C. System availability
Requests to emergency services are often critical in nature, and it's important for a dispatching system to always be available when a call is made.

The incorrect answers:
A. Integration costs
When lives are on the line, the cost is not commonly the most important aspect of a system integration.

B. Patch availability
Although it's important to always keep systems patched, it's more important that a life saving service be available to those who might need it.

D. Power usage
Power usage is not usually the most important consideration when building a critical healthcare and emergency service infrastructure.

More information:
SY0-701, Objective 3.1 - Infrastructure Considerations
https://professormesser.link/701030104

A11. A system administrator receives a text alert when access rights are changed on a database containing private customer information. Which of the following would describe this alert?

- ❍ **A.** Maintenance window
- ❍ **B.** Attestation and acknowledgment
- ❍ **C.** Automation
- ❍ **D.** External audit

The Answer: C. Automation
Automation ensures that compliance checks can be performed on a regular basis without the need for human intervention. This can be especially useful to provide alerts when a configuration change causes an organization to be out of compliance.

The incorrect answers:
A. Maintenance window
A maintenance window describes the scheduling associated with the change control process. Systems and services generally have limited availability during a maintenance window.

B. Attestation and acknowledgment
With compliance, the process of attestation and acknowledgment is the final verification of the formal compliance documentation. An alert from an automated process would not qualify as attestation.

D. External audit
An external audit can be a valuable tool for verifying the compliance process, but an automated alert from a monitoring system would not be part of an external audit.

More information:
SY0-701, Objective 5.4 - Compliance
https://professormesser.link/701050401

A12. A security administrator is concerned about the potential for data exfiltration using external storage drives. Which of the following would be the BEST way to prevent this method of data exfiltration?

- ❍ **A.** Create an operating system security policy to block the use of removable media
- ❍ **B.** Monitor removable media usage in host-based firewall logs
- ❍ **C.** Only allow applications that do not use removable media
- ❍ **D.** Define a removable media block rule in the UTM

The Answer: A. Create an operating system security policy to prevent the use of removable media

Removable media uses hot-pluggable interfaces such as USB to connect storage drives. A security policy in the operating system can prevent any files from being written to a removable drive.

The incorrect answers:
B. Monitor removable media usage in host-based firewall logs
A host-based firewall monitors traffic flows and does not commonly log hardware or USB drive access.

C. Only allow applications that do not use removable media
File storage access options are not associated with applications, so it's not possible to allow based on external storage drive usage.

D. Define a removable media block rule in the UTM
A UTM (Unified Threat Manager) watches traffic flows across the network and does not commonly manage the storage options on individual computers.

More information:
SY0-701, Objective 2.2 - Common Threat Vectors
https://professormesser.link/701020201

A13. A company creates a standard set of government reports each calendar quarter. Which of the following would describe this type of data?

- ❍ **A.** Data in use
- ❍ **B.** Obfuscated
- ❍ **C.** Trade secrets
- ❍ **D.** Regulated

The Answer: D. Regulated
Reports and information created for governmental use are regulated by laws regarding the disclosure of certain types of data.

The incorrect answers:
A. Data in use
Data in use describes information actively processing in the memory of a system, such as system RAM, CPU registers, or CPU cache. Government reports are static documents and are not actively being processed.

B. Obfuscated
Obfuscation describes the modification of data to make something understandable into something very difficult to understand. Information contained in a government report is relatively easy to understand and would not be considered obfuscated data.

C. Trade secrets
Trade secrets are the private details a company uses as part of their normal business processes, and these trade secrets are not shared with any other organization or business.

More information:
SY0-701, Objective 3.3 - Data Types and Classifications
https://professormesser.link/701030301

A14. An insurance company has created a set of policies to handle data breaches. The security team has been given this set of requirements based on these policies:

- Access records from all devices must be saved and archived
- Any data access outside of normal working hours must be immediately reported
- Data access must only occur inside of the country
- Access logs and audit reports must be created from a single database

Which of the following should be implemented by the security team to meet these requirements? (Select THREE)

❍ **A.** Restrict login access by IP address and GPS location

❍ **B.** Require government-issued identification during the onboarding process

❍ **C.** Add additional password complexity for accounts that access data

❍ **D.** Conduct monthly permission auditing

❍ **E.** Consolidate all logs on a SIEM

❍ **F.** Archive the encryption keys of all disabled accounts

❍ **G.** Enable time-of-day restrictions on the authentication server

---

The Answer: A. Restrict login access by IP address and GPS location,
E. Consolidate all logs on a SIEM, and
G. Enable time-of-day restrictions on the authentication server

Adding location-based policies will prevent direct data access from outside of the country. Saving log information from all devices and creating audit reports from a single database can be implemented through the use of a SIEM (Security Information and Event Manager). Adding a check for the time-of-day will report any access that occurs during non-working hours.

The incorrect answers:
B. Require government-issued identification during the onboarding process

Requiring proper identification is always a good idea, but it's not one of the listed requirements.

C. Add additional password complexity for accounts that access data
Additional password complexity is another good best practice, but it's not part of the provided requirements.

D. Conduct monthly permission auditing
No requirements for ongoing auditing were included in the requirements, but ongoing auditing is always an important consideration.

F. Archive the encryption keys of all disabled accounts
If an account is disabled, there may still be encrypted data that needs to be recovered later. Archiving the encryption keys will allow access to that data after the account is no longer in use.

More information:
SY0-701, Objective 4.6 - Access Controls
https://professormesser.link/701040602

A15. A security engineer, is viewing this record from the firewall logs:

```
UTC 04/05/2023 03:09:15809   AV Gateway Alert
136.127.92.171  80 -> 10.16.10.14  60818
Gateway Anti-Virus Alert:
XPACK.A_7854 (Trojan) blocked.
```

Which of the following can be observed from this log information?

- ❍ **A.** The victim's IP address is 136.127.92.171
- ❍ **B.** A download was blocked from a web server
- ❍ **C.** A botnet DDoS attack was blocked
- ❍ **D.** The Trojan was blocked, but the file was not

The Answer: B. A download was blocked from a web server
A traffic flow from a web server port number (80) to a device port (60818) indicates that this traffic flow originated on port 80 of the web server. A file download is one of the most common ways to deliver a Trojan, and this log entry shows that the file containing the XPACK.A_7854 Trojan was blocked.

The incorrect answers:
A. The victim's IP address is 136.127.92.171
The format for this log entry uses an arrow to differentiate between the attacker and the victim. The attacker IP address is 136.127.92.171, and the victim's IP address is 10.16.10.14.

C. A botnet DDoS attack was blocked
A botnet attack would not commonly include a Trojan horse as part of a distributed denial of service (DDoS) attack.

D. The Trojan was blocked, but the file was not
A Trojan horse attack involves malware that is disguised as legitimate software. The Trojan malware and the file are the same entity, so there isn't a way to decouple the malware from the file.

More information:
SY0-701, Objective 4.9 - Log Files
https://professormesser.link/701040901

A16. A user connects to a third-party website and receives this message:

```
Your connection is not private.
NET::ERR_CERT_INVALID
```

Which of the following attacks would be the MOST likely reason for this message?

- ❍ **A.** Brute force
- ❍ **B.** DoS
- ❍ **C.** On-path
- ❍ **D.** Deauthentication

The Answer: C. On-path
An on-path attack is often associated with a third-party who is actively intercepting network traffic. This entity in the middle would not be able to provide a valid SSL certificate for a third-party website, and this error would appear in the browser as a warning.

The incorrect answers:
A. Brute force
A brute force attack is commonly associated with password hacks. Brute force attacks would not cause the certificate on a website to be invalid.

B. DoS
A DoS (Denial of Service) attack would prevent communication to a server and most likely provide a timeout error. This error is not related to a service availability issue.

D. Deauthentication
Deauthentication attacks are commonly associated with wireless networks, and they usually cause disconnects and lack of connectivity. The error message in this example does not appear to be associated with a network outage or disconnection.

More information:
SY0-701, Objective 2.4 - On-Path Attacks
https://professormesser.link/701020409

A17. Which of the following would be the BEST way to provide a website login using existing credentials from a third-party site?

- ❍ **A.** Federation
- ❍ **B.** 802.1X
- ❍ **C.** EAP
- ❍ **D.** SSO

The Answer: A. Federation
Federation would allow members of one organization to authenticate using the credentials of another organization.

The incorrect answers:
B. 802.1X
802.1X is a useful authentication protocol, but it needs additional functionality to authenticate across multiple user databases.

C. EAP
EAP (Extensible Authentication Protocol) is an authentication framework commonly associated with network access control. EAP by itself does not provide the federation needed to authenticate users to a third-party access database.

D. SSO
SSO (Single Sign-On) describes the process of enabling a single authentication to grant access to many different network services. Obtaining login credentials from a third-party access database does not describe the process used by SSO.

More information:
SY0-701, Objective 4.6 - Identity and Access Management
https://professormesser.link/701040601

A18. A system administrator is working on a contract that will specify a minimum required uptime for a set of Internet-facing firewalls. The administrator needs to know how often the firewall hardware is expected to fail between repairs. Which of the following would BEST describe this information?

- ❍ **A.** MTBF
- ❍ **B.** RTO
- ❍ **C.** MTTR
- ❍ **D.** RPO

The Answer: A. MTBF
The MTBF (Mean Time Between Failures) is a prediction of how often a repairable system will fail.

The incorrect answers:
B. RTO
RTO (Recovery Time Objectives) define a timeframe needed to restore a particular service level.

C. MTTR
MTTR (Mean Time to Restore) is the amount of time it takes to repair a component.

D. RPO
RPO (Recovery Point Objective) describes the minimum data or operational state required to categorize a system as recovered.

More information:
SY0-701, Objective 5.2 - Business Impact Analysis
https://professormesser.link/701050204

A19. An attacker calls into a company's help desk and pretends to be the director of the company's manufacturing department. The attacker states that they have forgotten their password and they need to have the password reset quickly for an important meeting. What kind of attack would BEST describe this phone call?

- ❍ **A.** Social engineering
- ❍ **B.** Supply chain
- ❍ **C.** Watering hole
- ❍ **D.** On-path

The Answer: A. Social engineering
This social engineering attack uses impersonation to take advantage of authority and urgency principles in an effort to convince someone else to circumvent normal security controls.

The incorrect answers:
B. Supply chain
A supply chain attack focuses on the equipment or raw materials used to deliver products or services to an organization or user. A call to the help desk would not be categorized as part of the supply chain.

C. Watering hole
A watering hole attack uses a third-party site to perform attacks outside of a user's local (and usually more secure) network.

D. On-path
An on-path attack commonly occurs without any knowledge to the parties involved, and there's usually no additional notification that an attack is underway. In this question, the attacker contacted the help desk engineer directly.

More information:
SY0-701, Objective 2.2 - Impersonation
https://professormesser.link/701020203

A20. Two companies have been working together for a number of months, and they would now like to qualify their partnership with a broad formal agreement between both organizations. Which of the following would describe this agreement?

❍ **A.** SLA
❍ **B.** SOW
❍ **C.** MOA
❍ **D.** NDA

The Answer: C. MOA
An MOA (Memorandum of Agreement) is a formal document where both sides agree to a broad set of goals and objectives associated with the partnership.

The incorrect answers:
A. SLA
An SLA (Service Level Agreement) is commonly provided as a formal contract between two parties that documents the minimum terms for services provided. The SLA often provides very specific requirements and expectations between both parties.

B. SOW
An SOW (Statement of Work) is a detailed list of items to be completed as part of overall project deliverables. For example, a list of expected job tasks associated with a firewall installation would be documented in an SOW.

D. NDA
An NDA (Non-Disclosure Agreement) is a confidentiality agreement between parties. This question did not mention any requirement for privacy or confidentiality.

More information:
SY0-701, Objective 5.3 - Agreement Types
https://professormesser.link/701050302

A21. Which of the following would explain why a company would automatically add a digital signature to each outgoing email message?

- ❍ **A.** Confidentiality
- ❍ **B.** Integrity
- ❍ **C.** Authentication
- ❍ **D.** Availability

The Answer: B. Integrity
Integrity refers to the trustworthiness of data. A digital signature allows the recipient to confirm that none of the data has been changed since the digital signature was created.

The incorrect answers:
A. Confidentiality
Confidentiality describes the privacy of data. Encrypting traffic sent over a VPN or encrypting files stored on a flash drive would be an example of data confidentiality.

C. Authentication
Authentication refers to the process of verifying the identity of an individual or system. A username and password is a common method of authentication, but digital signatures are not commonly used as an authentication method.

D. Availability
Availability describes the ability of an authorized user to access data. A digital signature does not provide any features associated with the availability of the data.

More information:
SY0-701, Objective 1.2 - The CIA Triad
https://professormesser.link/701010201

A22. The embedded OS in a company's time clock appliance is configured to reset the file system and reboot when a file system error occurs. On one of the time clocks, this file system error occurs during the startup process and causes the system to constantly reboot. Which of the following BEST describes this issue?

- ❍ **A.** Memory injection
- ❍ **B.** Resource consumption
- ❍ **C.** Race condition
- ❍ **D.** Malicious update

The Answer: C. Race condition
A race condition occurs when two processes occur at similar times, and usually with unexpected results. The file system problem can often be fixed before a reboot, but the reboot is occurring before the fix can be applied. This has created a race condition that results in constant reboots.

The incorrect answers:
A. Memory injection
A memory injection is commonly used by malicious software to add code to the memory of an existing process. The issue in this question was related to a file system error and was not part of a malicious data injection.

B. Resource consumption
If the time clock was running out of storage space or memory, it would most likely be unusable. In this example, the issue isn't based on a lack of resources.

D. Malicious update
A malicious update occurs when a software patch installs unwanted or unauthorized code. Many attackers will use software patches to install their own malicious code during a software update.

More information:
SY0-701, Objective 2.3 - Race Conditions
https://professormesser.link/701020303

A23. A recent audit has found that existing password policies do not include any restrictions on password attempts, and users are not required to periodically change their passwords. Which of the following would correct these policy issues? (Select TWO)

- ❍ **A.** Password complexity
- ❍ **B.** Password expiration
- ❍ **C.** Password reuse
- ❍ **D.** Account lockout
- ❍ **E.** Password managers

The Answer: B. Password expiration and **D.** Account lockout
Password expiration would require a password change after the expiration date. An account lockout would disable an account after a predefined number of unsuccessful login attempts.

The incorrect answers:
A. Password complexity
A complex password would make the password more difficult to brute force, but it would not solve the issues listed in this question.

C. Password reuse
Maintaining a password history would prevent the reuse of any previous passwords. Restricting password reuse would ensure that a different password is used each time a password change is processed.

E. Password managers
A password manager would provide a way to securely store and retrieve passwords, but it would not resolve any issues relating to password expirations or account lockouts.

More information:
SY0-701, Objective 4.6 - Password Security
https://professormesser.link/701040604

A24. What kind of security control is associated with a login banner?

- ❍ **A.** Preventive
- ❍ **B.** Deterrent
- ❍ **C.** Corrective
- ❍ **D.** Detective
- ❍ **E.** Compensating
- ❍ **F.** Directive

The Answer: B. Deterrent
A deterrent control does not directly stop an attack, but it may discourage an action.

The incorrect answers:
A. Preventive
A preventive control physically limits access to a device or area.

C. Corrective
A corrective control can actively work to mitigate any damage.

D. Detective
A detective control may not prevent access, but it can identify and record any intrusion attempts.

E. Compensating
A compensating security control doesn't prevent an attack, but it does restore from an attack using other means.

F. Directive
A directive control is relatively weak control which relies on security compliance from the end users.

More information:
SY0-701, Objective 1.1 - Security Controls
https://professormesser.link/701010101

A25. An internal audit has discovered four servers that have not been updated in over a year, and it will take two weeks to test and deploy the latest patches. Which of the following would be the best way to quickly respond to this situation in the meantime?

- ❍ **A.** Purchase cybersecurity insurance
- ❍ **B.** Implement an exception for all data center services
- ❍ **C.** Move the servers to a protected segment
- ❍ **D.** Hire a third-party to perform an extensive audit

The Answer: C. Move the servers to a protected segment
Segmenting the servers to their own protected network would allow for additional security controls while still maintaining the uptime and availability of the systems.

The incorrect answers:
A. Purchase cybersecurity insurance
Cybersecurity insurance can help plan for financial issues during a significant attack, but it wouldn't provide any assistance for mitigating potential vulnerabilities during this two week period.

B. Implement an exception for all data center services
Security exceptions should be rare, and they should be very specific to a small number of systems. It would be risky to create a broad security exception for systems which are not in-scope for the identified vulnerability.

D. Hire a third-party to perform an extensive audit
Audits take time, and hiring a third-party to perform an audit takes even longer. By the time a third-party audit was underway, the problematic systems would have already been tested and patched.

More information:
SY0-701, Objective 4.3 - Vulnerability Remediation
https://professormesser.link/701040305

A26. A business manager is documenting a set of steps for processing orders if the primary Internet connection fails. Which of these would BEST describe these steps?

- ❍ **A.** Platform diversity
- ❍ **B.** Continuity of operations
- ❍ **C.** Cold site recovery
- ❍ **D.** Tabletop exercise

The Answer: B. Continuity of operations
It's always useful to have an alternative set of processes to handle any type of outage or issue. Continuity of operations planning ensures that the business will continue to operate when these issues occur.

The incorrect answers:
A. Platform diversity
Using different operating systems and platforms can help mitigate issues associated with a single OS, but it wouldn't provide any mitigation if the primary Internet connection was no longer available.

C. Cold site recovery
A cold site takes time to build, and the time and expense associated with a disaster recovery switchover would be extensive. By the time a cold site was enabled, the primary Internet connection may already be restored and many alternative recovery options could have potentially been deployed.

D. Tabletop exercise
A tabletop exercise usually consists of a meeting where members of a recovery team or disaster recovery talk through a disaster scenario.

More information:
SY0-701, Objective 3.4 - Resiliency
https://professormesser.link/701030401

A27. A company would like to examine the credentials of each individual entering the data center building. Which of the following would BEST facilitate this requirement?

- ❍ **A.** Access control vestibule
- ❍ **B.** Video surveillance
- ❍ **C.** Pressure sensors
- ❍ **D.** Bollards

The Answer: A. Access control vestibule
An access control vestibule is a room designed to restrict the flow of individuals through an area. These are commonly used in high security areas where each person needs to be evaluated and approved before access can be provided.

The incorrect answers:
B. Video surveillance
Although video surveillance can assist with monitoring access to a building or room, it doesn't provide a way to validate the credentials of each visitor.

C. Pressure sensors
Pressure sensors are commonly used on doors or windows to detect movement in those devices. However, pressure sensors would not be used to check visitor credentials.

D. Bollards
Bollards and barricades are often used on the exterior of a facility to prevent access to motorized vehicles and channel people through a specific access location.

More information:
SY0-701, Objective 1.2 - Physical Security
https://professormesser.link/701010206

A28. A company stores some employee information in encrypted form, but other public details are stored as plaintext. Which of the following would BEST describe this encryption strategy?

- ❍ **A.** Full-disk
- ❍ **B.** Record
- ❍ **C.** Asymmetric
- ❍ **D.** Key escrow

The Answer: B. Record
Record-level encryption is commonly used with databases to encrypt individual columns within the database. This would store some information in the database as plaintext and other information as encrypted data.

The incorrect answers:
A. Full-disk
Full-disk encryption ensures that all data on a storage drive is protected. Full-disk encryption protects all data on the drive, and none of the information would remain as the original plaintext.

C. Asymmetric
Asymmetric encryption uses a public and private key pair to encrypt data. Asymmetric encryption does not store some information as plaintext and other information as encrypted data.

D. Key escrow
Key escrow describes the storage and management of decryption keys by a third-party. Key escrow does not determine which data is selected for encryption or the method of encryption.

More information:
SY0-701, Objective 1.4 - Encrypting Data
https://professormesser.link/701010402

A29. A company would like to minimize database corruption if power is lost to a server. Which of the following would be the BEST strategy to follow?

- ❍ **A.** Encryption
- ❍ **B.** Off-site backups
- ❍ **C.** Journaling
- ❍ **D.** Replication

The Answer: C. Journaling
Journaling writes data to a temporary journal before writing the information to the database. If power is lost, the system can recover the last transaction from the journal when power is restored.

The incorrect answers:
A. Encryption
Encryption would provide confidentiality of the data, but it would not provide any additional integrity features if power was lost.

B. Off-site backups
Off-site backups can be used to recover a corrupted database, but this does not minimize or prevent database corruption from occurring.

D. Replication
Replication is used to create a duplicate copy of data. Although this process does provide a backup, it doesn't add any additional integrity and could still potentially corrupt data if power is lost.

More information:
SY0-701, Objective 3.4 - Backups
https://professormesser.link/701030404

A30. A company is creating a security policy for corporate mobile devices:

- All mobile devices must be automatically locked after a predefined time period.
- The location of each device needs to be traceable.
- All of the user's information should be completely separate from company data.

Which of the following would be the BEST way to establish these security policy rules?

❍ **A.** Segmentation

❍ **B.** Biometrics

❍ **C.** COPE

❍ **D.** MDM

The Answer: D. MDM
An MDM (Mobile Device Manager) provides a centralized management system for all mobile devices. From this central console, security administrators can set policies for many different types of mobile devices.

The incorrect answers:
A. Segmentation
Segmentation describes the separation of user data from company data, but the implementation all policies is managed by the MDM.

B. Biometrics
Biometrics can be used as another layer of device security, but you need more than biometrics to implement the required security policies in this question.

C. COPE
A device that is COPE (Corporately Owned and Personally Enabled) is commonly purchased by the corporation and allows the use of the mobile device for both business and personal use. The use of a COPE device does not provide any policy management of the device.

More information:
SY0-701, Objective 4.1 - Securing Wireless and Mobile
https://professormesser.link/701040103

A31. A security engineer runs a monthly vulnerability scan. The scan doesn't list any vulnerabilities for Windows servers, but a significant vulnerability was announced last week and none of the servers are patched yet. Which of the following best describes this result?

- ❍ **A.** Exploit
- ❍ **B.** Compensating controls
- ❍ **C.** Zero-day attack
- ❍ **D.** False negative

The Answer: D. False negative
A false negative is a result that fails to detect an issue when one actually exists.

The incorrect answers:
A. Exploit
An exploit is an attack against a vulnerability. Vulnerability scans do not commonly attempt to exploit the vulnerabilities that they identify.

B. Compensating controls
Compensating controls are used to mitigate a vulnerability when an optimal security response may not be available. For example, if a company can't deploy a patch for a vulnerability, they can revoke or limit application access until a patch is provided.

C. Zero-day attack
A zero-day attack focuses on previously unknown vulnerabilities. In this example, the vulnerability scan isn't an attack, and the vulnerabilities are already known and patches are available.

More information:
SY0-701, Objective 4.3 - Analyzing Vulnerabilities
https://professormesser.link/701040304

A32. An IT help desk is using automation to improve the response time for security events. Which of the following use cases would apply to this process?

- ❍ **A.** Escalation
- ❍ **B.** Guard rails
- ❍ **C.** Continuous integration
- ❍ **D.** Resource provisioning

The Answer: A. Escalation
Automation can recognize security events and escalate a security-related ticket to the incident response team without any additional human interaction.

The incorrect answers:
B. Guard rails
Guard rails are used by application developers to provide a set of automated validations to user input and behavior. Guard rails are not used by the help desk team.

C. Continuous integration
Continuous integration and testing provides an automated method of constantly developing, testing, and deploying code. The continuous integration process is not used by the help desk.

D. Resource provisioning
Resource provisioning can be automated during the on-boarding and off-boarding process to quickly create or remove rights and permissions. Resource provisioning is not commonly part of the automation associated with security event notification.

More information:
SY0-701, Objective 4.7 - Scripting and Automation
https://professormesser.link/701040701

A33. A network administrator would like each user to authenticate with their corporate username and password when connecting to the company's wireless network. Which of the following should the network administrator configure on the wireless access points?

- ❍ **A.** WPA3
- ❍ **B.** 802.1X
- ❍ **C.** PSK
- ❍ **D.** MFA

The Answer: B. 802.1X
802.1X uses a centralized authentication server, and this allows all users to use their corporate credentials during the login process.

The incorrect answers:
A. WPA3
WPA3 (Wi-Fi Protected Access 3) is an encryption protocol for 802.11 wireless networking. The WPA3 encryption itself does not include the centralized authentication process described in this question.

C. PSK
PSK (Pre-Shared Key) is a wireless configuration option that allows everyone on the network to use the same access key or password when connecting to the wireless network. This question requires each person to use unique authentication credentials.

D. MFA
MFA (Multifactor Authentication) describes the use of multiple types of authentication checks. A username and password is a single factor (something you know), and the use of MFA does not itself require unique username and password credentials for each user.

More information:
SY0-701, Objective 3.2 - Port Security
https://professormesser.link/701030205

A34. A company's VPN service performs a posture assessment during the login process. Which of the following mitigation techniques would this describe?

- ❍ **A.** Encryption
- ❍ **B.** Decommissioning
- ❍ **C.** Least privilege
- ❍ **D.** Configuration enforcement

The Answer: D. Configuration enforcement
A posture assessment evaluates the configuration of a system to ensure all configurations and applications are up to date and secure as possible. If a configuration does not meet these standards, the user is commonly provided with options for resolving the issue before proceeding.

The incorrect answers:
A. Encryption
Encryption is an important part of a VPN (Virtual Private Network), but the encryption of network data is not related to the posture assessment process.

B. Decommissioning
It's important to properly manage data during any decommissioning process, but the decommissioning isn't part of the VPN login process.

C. Least privilege
Least privilege describes the minimum rights and permissions that would allow an individual to perform their job function. Least privilege is not part of a posture assessment.

More information:
SY0-701, Objective 2.5 - Mitigation Techniques
https://professormesser.link/701020502

A35. A user has assigned individual rights and permissions to a file on their network drive. The user adds three additional individuals to have read-only access to the file. Which of the following would describe this access control model?

❍ **A.** Discretionary

❍ **B.** Mandatory

❍ **C.** Attribute-based

❍ **D.** Role-based

The Answer: A. Discretionary
Discretionary access control is used in many operating systems, and this model allows the owner of the resource to control who has access.

The incorrect answers:
B. Mandatory
Mandatory access control allows access based on the security level assigned to an object. Only users with the object's assigned security level or higher may access the resource.

C. Attribute-based
Attribute-based access control combines many different parameters to determine if a user has access to a resource.

D. Role-based
Role-based access control assigns rights and permissions based on the role of a user. These roles are usually assigned by group.

More information:
SY0-701, Objective 4.6 - Access Controls
https://professormesser.link/701040602

A36. A remote user has received a text message with a link to login and confirm their upcoming work schedule. Which of the following would BEST describe this attack?

- ❍ **A.** Brute force
- ❍ **B.** Watering hole
- ❍ **C.** Typosquatting
- ❍ **D.** Smishing

The Answer: D. Smishing
Smishing, or SMS (Short Message Service) phishing, is a social engineering attack that asks for sensitive information using SMS or text messages.

The incorrect answers:
A. Brute force
A brute force attack tries multiple password combinations in an effort to identify the correct authentication details.

B. Watering hole
A watering hole attack will infect a third-party site visited by the victim. Watering hole attacks are not commonly associated with received text messages.

C. Typosquatting
Typosquatting uses a misspelling of a domain name to convince victims they are visiting a legitimate website. The information provided in this question does not provide any specific domain names or links.

More information:
SY0-701, Objective 2.2 - Phishing
https://professormesser.link/701020202

A37. A company is formalizing the design and deployment process used by their application programmers. Which of the following policies would apply?

- ❍ **A.** Business continuity
- ❍ **B.** Acceptable use policy
- ❍ **C.** Incident response
- ❍ **D.** Development lifecycle

The Answer: D. Development lifecycle
A formal software development lifecycle defines the specific policies associated with the design, development, testing, deployment, and maintenance of the application development process.

The incorrect answers:
A. Business continuity
Business continuity plans define the procedures used when the primary business systems are unavailable. The business continuity process is not commonly associated with the application development process.

B. Acceptable use policy
An acceptable use policy formally defines the proper use of company assets and technology devices.

C. Incident response
Incident response policies define the procedures to follow when a security incident is identified. Incident response is not part of the application development process

More information:
SY0-701, Objective 5.1 - Security Policies
https://professormesser.link/701050101

A38. A security administrator has copied a suspected malware executable from a user's computer and is running the program in a sandbox. Which of the following would describe this part of the incident response process?

- ❍ **A.** Eradication
- ❍ **B.** Preparation
- ❍ **C.** Recovery
- ❍ **D.** Containment

.....

The Answer: D. Containment
The isolation and containment process prevents malware from spreading and allows the administrator to analyze the operation of the malware without putting any other devices at risk.

The incorrect answers:
A. Eradication
The eradication phase is associated with completely removing malware from a system. This process usually involves removing all data from a system and installing or re-imaging with a known-good operating system.

B. Preparation
The preparation process occurs before a security incident is discovered, and it can include the documentation of communication methods, the compiling of mitigation software, or gathering network and application documentation.

C. Recovery
The recovery phase is associated with the recovery of a system after a security incident. Running malware in a sandbox is not part of the recovery process.

More information:
SY0-701, Objective 4.8 - Incident Response
https://professormesser.link/701040801

A39. A server administrator at a bank has noticed a decrease in the number of visitors to the bank's website. Additional research shows that users are being directed to a different IP address than the bank's web server. Which of the following would MOST likely describe this attack?

- ❍ **A.** Deauthentication
- ❍ **B.** DDoS
- ❍ **C.** Buffer overflow
- ❍ **D.** DNS poisoning

The Answer: D. DNS poisoning
A DNS poisoning can modify a DNS server to modify the IP address provided during the name resolution process. If an attacker modifies the DNS information, they can direct client computers to any destination IP address.

The incorrect answers:
A. Deauthentication
Deauthentication attacks are commonly associated with wireless networks. The deauthentication attack is used to remove devices from the wireless network, and it does not commonly redirect clients to a different website.

B. DDoS
A DDoS (Distributed Denial of Service) is used by attackers to cause services to be unavailable. In this example, the bank's website is operational but clients are not resolving the correct IP address.

C. Buffer overflow
Buffer overflows are associated with application attacks and can cause applications to crash or act in unexpected ways. A buffer overflow would not commonly redirect clients to a different website IP address.

More information:
SY0-701, Objective 2.4 - DNS Attacks
https://professormesser.link/701020407

A40. Which of the following considerations are MOST commonly associated with a hybrid cloud model?

- ❍ **A.** Microservice outages
- ❍ **B.** IoT support
- ❍ **C.** Network protection mismatches
- ❍ **D.** Containerization backups

The Answer: C. Network protection mismatches
A hybrid cloud includes more than one private or public cloud. This adds additional complexity to the overall infrastructure, and it's common to inadvertently apply different authentication options and user permissions across multiple cloud providers.

The incorrect answers:
A. Microservice outages
Microservices are used to create a scalable and resilient application instance. However, the availability of a microservice is not specific to a hybrid cloud model.

B. IoT support
IoT (Internet of Things) support is available in many cloud infrastructure models, and this would not be specific to a hybrid cloud.

D. Containerization backups
Containerization provides an efficient method of deploying application instances, but the use and backup of these containers is not specific to a hybrid cloud infrastructure.

More information:
SY0-701, Objective 3.1 - Cloud Infrastructures
https://professormesser.link/701030101

A41. A company hires a large number of seasonal employees, and their system access should normally be disabled when the employee leaves the company. The security administrator would like to verify that their systems cannot be accessed by any of the former employees. Which of the following would be the BEST way to provide this verification?

- ❍ **A.** Confirm that no unauthorized accounts have administrator access
- ❍ **B.** Validate the account lockout policy
- ❍ **C.** Validate the offboarding processes and procedures
- ❍ **D.** Create a report that shows all authentications for a 24-hour period

---

The Answer: C. Validate the offboarding processes and procedures
The disabling of an employee account is commonly part of the offboarding process. One way to validate an offboarding policy is to perform an audit of all accounts and compare active accounts with active employees.

The incorrect answers:
A. Confirm that no unauthorized accounts have administrator access
It's always a good idea to periodically audit administrator accounts, but this audit won't provide any validation that all former employee accounts have been disabled.

B. Validate the account lockout policy
Account lockouts occur when a number of invalid authentication attempts have been made to a valid account. Disabled accounts would not be locked out because they are not currently valid accounts.

D. Create a report that shows all authentications for a 24-hour period
A list of all authentications would be quite large, and it would not be obvious to see which authentications were made with valid accounts and which authentications were made with former employee accounts.

More information:
SY0-701, Objective 5.1 - Security Procedures
https://professormesser.link/701050103

A42. Which of the following is used to describe how cautious an organization might be to taking a specific risk?

- ❍ **A.** Risk appetite
- ❍ **B.** Risk register
- ❍ **C.** Risk transfer
- ❍ **D.** Risk reporting

The Answer: A. Risk appetite
A risk appetite is a broad description of how much risk-taking is deemed acceptable. An organization's risk appetite posture might be conservative, or they might be more expansionary and willing to take additional risks.

The incorrect answers:
B. Risk register
A risk register identifies and documents the risks associated with each step of a project plan. A risk register is not designed to describe an organization's level of caution associated with each risk.

C. Risk transfer
Some organizations will transfer their risk to a third-party. For example, many organizations will purchase cybersecurity insurance to minimize the financial impact of a cybersecurity event.

D. Risk reporting
Risk reporting is the formal process of identifying risk and documenting all details associated with the risk. These reports are commonly designed for the decision making process by the senior management of an organization.

More information:
SY0-701, Objective 5.2 - Risk Analysis
https://professormesser.link/701050202

A43. A technician is applying a series of patches to fifty web servers during a scheduled maintenance window. After patching and rebooting the first server, the web service fails with a critical error. Which of the following should the technician do NEXT?

- ❍ **A.** Contact the stakeholders regarding the outage
- ❍ **B.** Follow the steps listed in the backout plan
- ❍ **C.** Test the upgrade process in the lab
- ❍ **D.** Evaluate the impact analysis associated with the change

---

The Answer: B. Follow the steps listed in the backout plan
The backout plan associated with the change control process provides information on reverting to the previous configuration if an unrecoverable error is found during the change.

The incorrect answers:
A. Contact the stakeholders regarding the outage
The stakeholders don't commonly require a detailed notification of every step during the maintenance window. The final disposition of the change can be communicated to the stakeholders after the maintenance window has concluded.

C. Test the upgrade process in the lab
The testing phase of the change control process takes place prior to the maintenance window. Once the maintenance window has started, it's too late to perform any additional tests in the lab.

D. Evaluate the impact analysis associated with the change
An impact analysis determines the risk for making the proposed change. This analysis is created prior to the change control approval, and it would not be very useful when troubleshooting during the maintenance window.

More information:
SY0-701, Objective 1.3 - Change Management Process
https://professormesser.link/701010301

A44. An attacker has discovered a way to disable a server by sending specially crafted packets from many remote devices to the operating system. When the packet is received, the system crashes and must be rebooted to restore normal operations. Which of the following would BEST describe this attack?

- ❍ **A.** Privilege escalation
- ❍ **B.** SQL injection
- ❍ **C.** Replay attack
- ❍ **D.** DDoS

.....

The Answer: D. DDoS
A DDoS (Distributed Denial of Service) is an attack that overwhelms or disables a service to prevent the service from operating normally. Packets from multiple devices that disable a server would be an example of a DDoS attack.

The incorrect answers:
A. Privilege escalation
A privilege escalation attack allows a user to exceed their normal rights and permissions. In this example, user permission escalations were not required to perform this attack.

B. SQL injection
A SQL (Structured Query Language) injection is used to circumvent an application and communicate directly to the application's database. In this question, there was no mention of application vulnerabilities or specific SQL statements.

C. Replay attack
A replay attack captures information and then replays that information as the method of attack. In this question, no mention was made of a prior data capture.

More information:
SY0-701, Objective 2.4 - Denial of Service
https://professormesser.link/701020406

A45. A data breach has occurred in a large insurance company. A security administrator is building new servers and security systems to get all of the financial systems back online. Which part of the incident response process would BEST describe these actions?

- ❍ **A.** Lessons learned
- ❍ **B.** Containment
- ❍ **C.** Recovery
- ❍ **D.** Analysis

The Answer: C. Recovery
The recovery after a breach can be a phased approach that may take months to complete.

The incorrect answers:
A. Lessons learned
Once the event is over, it's useful to revisit the process to learn and improve for next time.

B. Containment
During an incident, it's useful to separate infected systems from the rest of the network.

D. Analysis
The analysis phase can include the analysis of log files and alerts. These data source can help warn of a potential attack or evidence an attack is underway.

More information:
SY0-701, Objective 4.8 - Incident Response
https://professormesser.link/701040801

A46. A network team has installed new access points to support an application launch. In less than 24 hours, the wireless network was attacked and private company information was accessed. Which of the following would be the MOST likely reason for this breach?

- ❍ **A.** Race condition
- ❍ **B.** Jailbreaking
- ❍ **C.** Impersonation
- ❍ **D.** Misconfiguration

The Answer: D. Misconfiguration
There are many different configuration options when installing an access point, and it's likely one of those options allowed an attacker to gain access to the internal network.

The incorrect answers:
A. Race condition
A race condition occurs when two different application processes are executing simultaneously. If the two processes are not aware of each other, the application may have unexpected results. In this example, there's no evidence the access points were experiencing a race condition.

B. Jailbreaking
Jailbreaking replaces the firmware on a mobile device to gain access to features not normally available in the operating system. Jailbreaking is not commonly associated with wireless access points.

C. Impersonation
Impersonation is an attacker pretending to be someone or something they are not. In this example, there's no evidence that impersonation was used to breach the wireless network.

More information:
SY0-701, Objective 2.3 - Misconfiguration Vulnerabilities
https://professormesser.link/701020313

A47. An organization has identified a significant vulnerability in an Internet-facing firewall. The firewall company has stated the firewall is no longer available for sale and there are no plans to create a patch for this vulnerability. Which of the following would BEST describe this issue?

- ❍ **A.** End-of-life
- ❍ **B.** Improper input handling
- ❍ **C.** Improper key management
- ❍ **D.** Incompatible OS

The Answer: A. End-of-life
Because the firewall is no longer available for sale, the firewall company has decided to stop supporting and updating the device. A product no longer supported by the manufacturer is consider to be end-of-life.

The incorrect answers:
B. Improper input handling
A best practice for application security is to provide the proper handling of invalid or unnecessary input. A missing patch for the firewall firmware would not be related to input handling.

C. Improper key management
Cryptographic keys can be used for many security purposes, but managing those keys isn't part of the patching process from a vendor.

D. Incompatible OS
The operating system in the firewall would normally be supported by the manufacturer, and the operating systems are not commonly modified on a purpose-built device such as a firewall.

More information:
SY0-701, Objective 2.3 - Hardware vulnerabilities
https://professormesser.link/701020308

A48. A company has decided to perform a disaster recovery exercise during an annual meeting with the IT directors and senior directors. A simulated disaster will be presented, and the participants will discuss the logistics and processes required to resolve the disaster. Which of the following would BEST describe this exercise?

- ❍ **A.** Capacity planning
- ❍ **B.** Business impact analysis
- ❍ **C.** Continuity of operations
- ❍ **D.** Tabletop exercise

The Answer: D. Tabletop exercise
A tabletop exercise allows a disaster recovery team to evaluate and plan disaster recovery processes without performing a full-scale drill.

The incorrect answers:
A. Capacity planning
Capacity planning is used to determine how many resources would be required for a particular task. A formal tabletop exercise would not commonly include a capacity planning analysis.

B. Business impact analysis
A business impact analysis is usually created during the disaster recovery planning process. Once the disaster has occurred, it becomes much more difficult to complete an accurate impact analysis.

C. Continuity of operations
If an outage occurs, it's common to have a backup plan to provide continuity of operations. This plan can be used for any significant outage and is not specific to disaster recovery testing.

More information:
SY0-701, Objective 3.4 - Recovery Testing
https://professormesser.link/701030403

A49. A security administrator needs to block users from visiting websites hosting malicious software. Which of the following would be the BEST way to control this access?

- ❍ **A.** Honeynet
- ❍ **B.** Data masking
- ❍ **C.** DNS filtering
- ❍ **D.** Data loss prevention

The Answer: C. DNS filtering
DNS filtering uses a database of known malicious websites to resolve an incorrect or null IP address. If a user attempts to visit a known malicious site, the DNS resolution will fail and the user will not be able to visit the website.

The incorrect answers:
A. Honeynet
A honeynet is a non-production network created to attract attackers. A honeynet is not used to block traffic to known malicious Internet sites.

B. Data masking
Data masking provides a way to hide data by substitution, shuffling, encryption, and other methods. Data masking does not provide a method of blocking communication to malicious websites.

D. Data loss prevention
Data Loss Prevention (DLP) systems can identify and block private information from being transferred between systems. DLP does not provide any direct method of blocking network traffic to known malware repositories.

More information:
SY0-701, Objective 4.5 - Web Filtering
https://professormesser.link/701040502

A50. A system administrator has been called to a system with a malware infection. As part of the incident response process, the administrator has imaged the operating system to a known-good version. Which of these incident response steps is the administrator following?

- ❍ **A.** Lessons learned
- ❍ **B.** Recovery
- ❍ **C.** Detection
- ❍ **D.** Containment

.....

The Answer: B. Recovery
The recovery phase describes the process of returning the system and data to the state prior to the malware infection. With a malware infection, this often requires deleting all data and reinstalling a known-good operating system.

The incorrect answers:
A. Lessons learned
A post-incident meeting can help the incident response participants discuss the phases of the incident that went well and which processes can be improved for future events.

C. Detection
The detection of the malware is an early phase in the incident response process. If the administrator is imaging a system, the malware was previously detected and any critical documents were already recovered.

D. Containment
The containment phase isolates the system from any other devices to prevent the spread of any malicious software. The containment phase generally occurs immediately after

More information:
SY0-701, Objective 4.8 - Incident Response
https://professormesser.link/701040801

A51. A company has placed a SCADA system on a segmented network with limited access from the rest of the corporate network. Which of the following would describe this process?

- ❍ **A.** Load balancing
- ❍ **B.** Least privilege
- ❍ **C.** Data retention
- ❍ **D.** Hardening

The Answer: D. Hardening
The hardening process for an industrial SCADA (Supervisory Control and Data Acquisition) system might include network segmentation, additional firewall controls, and the implementation of access control lists.

The incorrect answers:
A. Load balancing
A load balancer is used to distribute transactions across multiple systems. A single system was the only device referenced in this question, so a load balancing option would not be available.

B. Least privilege
Least privilege defines the minimum rights and permissions for completing a specific task. In this example, there was no mention of specific tasks or their necessary permissions.

C. Data retention
Data retention is important for long-term storage of important information. In this example, the mandated storage of data was not a consideration.

More information:
SY0-701, Objective 4.1 - Hardening Targets
https://professormesser.link/701040102

A52. An administrator is viewing the following security log:

```
Dec 30 08:40:03 web01 Failed password for root
from 10.101.88.230 port 26244 ssh2

Dec 30 08:40:05 web01 Failed password for root
from 10.101.88.230 port 26244 ssh2

Dec 30 08:40:09 web01 445 more authentication
failures; rhost=10.101.88.230 user=root
```

Which of the following would describe this attack?

- ❍ **A.** Spraying
- ❍ **B.** Downgrade
- ❍ **C.** Brute force
- ❍ **D.** DDoS

The Answer: C. Brute force
A brute force attack discovers password by attempting a large combination of letters, numbers, and special characters until a match is found. In this example, the notification of over four hundred attempts would qualify as a brute force attack.

The incorrect answers:
A. Spraying
A spraying attack is similar to a brute force attack, but spraying limits the number of attempts to prevent alerts or an account lockout. A spraying attack often uses accounts passwords stolen from other sites or a short list of the most common passwords.

B. Downgrade
A downgrade attack is often used to force an insecure encryption algorithm or the disabling of encryption entirely. In this example, no evidence of a downgrade attack is contained in the security log.

D. DDoS
A DDoS (Distributed Denial of Service) would involve many different devices to cause a system outage. In this example, a single IP address was logged and there was no evidence of a service outage.

More information:
SY0-701, Objective 4.9 - Log data
https://professormesser.link/701040901

A53. During a morning login process, a user's laptop was moved to a private VLAN and a series of updates were automatically installed. Which of the following would describe this process?

- ❍ **A.** Account lockout
- ❍ **B.** Configuration enforcement
- ❍ **C.** Decommissioning
- ❍ **D.** Sideloading

The Answer: B. Configuration enforcement
Many organizations will perform a posture assessment during the login process to verify the proper security controls are in place. If the device does not pass the assessment, the system can be quarantined and any missing security updates can then be installed.

The incorrect answers:
A. Account lockout
In this example, there were no errors or notifications regarding the account or authentication status.

C. Decommissioning
The decommissioning process is often used to permanently remove devices from the network. In this example, the laptop mitigation would allow the device to return to the network once the updates were complete.

D. Sideloading
Sideloading describes the installation of software on a mobile device through the use of third-party operating systems or websites.

More information:
SY0-701, Objective 2.5 - Mitigation Techniques
https://professormesser.link/701020502

A54. Which of the following describes two-factor authentication?

- ❍ **A.** A printer uses a password and a PIN
- ❍ **B.** The door to a building requires a fingerprint scan
- ❍ **C.** An application requires a pseudo-random code
- ❍ **D.** A Windows Domain requires a password and smart card

.....

The Answer: D. A Windows Domain requires a password and smart card
The multiple factors of authentication for this Windows Domain are a password (something you know), and a smart card (something you have).

The incorrect answers:
A. A printer uses a password and a PIN
A password and a PIN (Personal Identification Number) are both something you know, so only one authentication factor is used.

B. The door to a building requires a fingerprint scan
A biometric scan (something you are) is a single factor of authentication.

C. An application requires a pseudo-random code
Pseudo-random authentication codes are often provided using a hardware dongle or mobile app. This single factor of authentication is something you have.

More information:
SY0-701, Objective 4.6 - Multi-factor Authentication
https://professormesser.link/701040603

A55. A company is deploying a new application to all employees in the field. Some of the problems associated with this roll out include:

- The company does not have a way to manage the devices in the field
- Team members have many different kinds of mobile devices
- The same device needs to be used for both corporate and private use

Which of the following deployment models would address these concerns?

❍ **A.** CYOD

❍ **B.** SSO

❍ **C.** COPE

❍ **D.** BYOD

The Answer: C. COPE
A COPE (Corporate-owned, Personally Enabled) device would solve the issue of device standardization and would allow the device to be used for both corporate access and personal use.

The incorrect answers:
A. CYOD
CYOD (Choose Your Own Device) allows the user to pick the make and model of their device. This would not solve the issue of different kinds of mobile devices used in the field.

B. SSO
SSO (Single Sign-On) is used to authenticate once when accessing multiple resources. SSO would not resolve any of the listed issues.

D. BYOD
With BYOD (Bring Your Own Device), the employee uses their personal device at work. This would not address the issue of mobile device management or standardization of mobile devices.

More information:
SY0-701, Objective 4.1 - Securing Wireless and Mobile
https://professormesser.link/701040103

A56. An organization is installing a UPS for their new data center. Which of the following would BEST describe this control type?

- ❍ **A.** Compensating
- ❍ **B.** Directive
- ❍ **C.** Deterrent
- ❍ **D.** Detective

The Answer: A. Compensating
A compensating security control doesn't prevent an attack, but it does restore from an attack using other means. In this example, the UPS (Uninterruptible Power Supply) does not stop a power outage, but it does provide alternative power if an outage occurs.

The incorrect answers:
B. Directive
A directive control provides security controls using instructions and guidance. A UPS is not categorized as a directive control.

C. Deterrent
A deterrent control discourages an intrusion attempt. A UPS is used after power has been lost, so it would not be categorized as a deterrent.

D. Detective
A detective control may not prevent access, but it can identify and record intrusion attempts.

More information:
SY0-701, Objective 1.1 - Security Controls
https://professormesser.link/701010101

A57. A manufacturing company would like to track the progress of parts used on an assembly line. Which of the following technologies would be the BEST choice for this task?

- ❍ **A.** Secure enclave
- ❍ **B.** Blockchain
- ❍ **C.** Hashing
- ❍ **D.** Asymmetric encryption

The Answer: B. Blockchain
The ledger functionality of a blockchain can be used to track or verify components, digital media, votes, and other physical or digital objects.

The incorrect answers:
A. Secure enclave
A secure enclave is a protected area for secret information, and the secure enclave is often implemented as a hardware processor in a device.

C. Hashing
Cryptographic hashes are commonly used to provide integrity verifications, but they don't necessarily include any method of tracking components on an assembly line.

D. Asymmetric encryption
Asymmetric encryption uses different keys for encryption and decryption. Asymmetric encryption does not provide any method for tracking objects on an assembly line.

More information:
SY0-701, Objective 1.4 - Blockchain Technology
https://professormesser.link/701010407

A58. A company's website has been compromised and the website content has been replaced with a political message. Which of the following threat actors would be the MOST likely culprit?

- ❍ **A.** Insider
- ❍ **B.** Organized crime
- ❍ **C.** Shadow IT
- ❍ **D.** Hacktivist

The Answer: D. Hacktivist
A hacktivist is motivated by a particular philosophy, and their goal is to spread their message by defacing web sites and releasing private documents.

The incorrect answers:
A. Insider
An insider has access to many company services, but the motivations of an insider threat would not commonly result in the posting of political information.

B. Organized crime
Organized crime actors are motivated by money. It would be unusual for an organized crime hack to include the posting of political messages.

C. Shadow IT
A shadow IT group is mostly interested in building their own systems and applications, and they would not commonly deface a website in an attempt to spread a specific political message.

More information:
SY0-701, Objective 2.1 - Threat Actors
https://professormesser.link/701020101

A59. A Linux administrator is downloading an updated version of her Linux distribution. The download site shows a link to the ISO and a SHA256 hash value. Which of these would describe the use of this hash value?

- ❍ **A.** Verifies that the file was not corrupted during the file transfer
- ❍ **B.** Provides a key for decrypting the ISO after download
- ❍ **C.** Authenticates the site as an official ISO distribution site
- ❍ **D.** Confirms that the file does not contain any malware

The Answer: A. Verifies that the file was not corrupted during the file transfer

Once the file is downloaded, the administrator can calculate the file's SHA256 hash and confirm that it matches the value on the website.

The incorrect answers:
B. Provides a key for decrypting the ISO after download
ISO files containing public information are usually distributed without any encryption, and a hash value would not commonly be used as a decryption key.

C. Authenticates the site as an official ISO distribution site
Although it's important to download files from known good sites, providing a hash value on a site would not provide any information about the site's authentication.

D. Confirms that the file does not contain any malware
A hash value doesn't inherently provide any protection against malware.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

A60. A company's security policy requires that login access should only be available if a person is physically within the same building as the server. Which of the following would be the BEST way to provide this requirement?

- ❍ **A.** USB security key
- ❍ **B.** Biometric scanner
- ❍ **C.** PIN
- ❍ **D.** SMS

The Answer: B. Biometric scanner
A biometric scanner would require a person to be physically present to verify the authentication.

The incorrect answers:
A. USB security key
A security key can be used to store a certificate on a USB (Universal Serial Bus) drive. The security key is commonly used as an authentication method for a user or application, and it doesn't provide any information about the location of the security key.

C. PIN
Although a PIN (Personal Identification Number) can be used as an authentication factor, the use of the PIN does not guarantee that a person is physically present.

D. SMS
SMS (Short Message Service), or text messages, are commonly used as authentication factors. However, the use of a mobile device to receive the SMS message does not guarantee that the owner of the mobile device is physically present.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

A61. A development team has installed a new application and database to a cloud service. After running a vulnerability scanner on the application instance, a security administrator finds the database is available for anyone to query without providing any authentication. Which of these vulnerabilities is MOST associated with this issue?

- ❍ **A.** Legacy software
- ❍ **B.** Open permissions
- ❍ **C.** Race condition
- ❍ **D.** Malicious update

The Answer: B. Open permissions
Just like local systems, proper permissions and security controls are required when applications are installed to a cloud-based system. If permissions are not properly configured, the application data may be accessible by anyone on the Internet.

The incorrect answers:
A. Legacy software
Legacy software often describes an older application with limited support options. The application and database in this example is a new installation and would not normally be categorized as legacy.

C. Race condition
If two processes occur simultaneously without coordination between the processes, unexpected results could occur. In this example, a single vulnerability scan has identified the issue and other processes do not appear to be involved.

D. Malicious update
A malicious update involves the installation of unwanted software during a normal update process. In this example, an update was not performed and the resulting public access would not generally be part of a malicious update.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

A62. Employees of an organization have received an email with a link offering a cash bonus for completing an internal training course. Which of the following would BEST describe this email?

- ❍ **A.** Watering hole attack
- ❍ **B.** Cross-site scripting
- ❍ **C.** Zero-day
- ❍ **D.** Phishing campaign

The Answer: D. Phishing campaign
A phishing campaign is an internal process used to test the security habits of the user community. An email with a link from a server not under the control of the company could be an email sent by the IT department as part of a phishing campaign.

The incorrect answers:
A. Watering hole attack
A watering hole attack is used as an alternative to attacking a victim's device directly. With a watering hole attack, an attacker will compromise a site used by the victim and will simply wait for the victim to visit.

B. Cross-site scripting
Cross-site scripting takes advantage of the trust already existing in a web browser. In this example, there's no evidence of a vulnerable web application or a specific browser-based vulnerability.

C. Zero-day
A zero-day attack describes a vulnerability where a software patch or similar mitigation is not immediately available. A link in an email by itself does not describe a zero-day attack.

More information:
SY0-701, Objective 5.6 - Security Awareness
https://professormesser.link/701050601

A63. Which of the following risk management strategies would include the purchase and installation of an NGFW?

- ❍ **A.** Transfer
- ❍ **B.** Mitigate
- ❍ **C.** Accept
- ❍ **D.** Avoid

The Answer: B. Mitigate
Mitigation is a strategy that decreases the threat level. This is commonly done through the use of additional security systems and monitoring, such as an NGFW (Next-Generation Firewall).

The incorrect answers:
A. Transfer
Transferring risk would move the risk from one entity to another. Adding an NGFW would not transfer any risk to another party.

C. Accept
The acceptance of risk is a position where the owner understands the risk and has decided to accept the potential results.

D. Avoidance
With risk avoidance, the owner of the risk decides to stop participating in a high-risk activity. This effectively avoids the risky activity and prevents any future issues.

More information:
SY0-701, Objective 3.2 - Firewall Types
https://professormesser.link/701030206

A64. An organization is implementing a security model where all application requests must be validated at a policy enforcement point. Which of the following would BEST describe this model?

- ❍ **A.** Public key infrastructure
- ❍ **B.** Zero trust
- ❍ **C.** Discretionary access control
- ❍ **D.** Federation

The Answer: B. Zero trust
Zero trust describes a model where nothing is inherently trusted and everything must be verified to gain access. A central policy enforcement point is commonly used to implement a zero trust architecture.

The incorrect answers:
A. Public key infrastructure
A public key infrastructure (PKI) uses public and private keys to provide confidentiality and integrity. Asymmetric encryption and digital signatures are used as foundational technologies in PKI.

C. Discretionary access control.
Discretionary access control is an authorization method where the owner of the data determines the scope and type of access. A discretionary access control model does not specifically define how the authorization is implemented.

D. Federation
Federation provides a way to manage authentication to a third-party database. Federation does not describe the use of a policy enforcement point.

More information:
SY0-701, Objective 1.2 - Zero Trust
https://professormesser.link/701010205

A65. A company is installing a new application in a public cloud. Which of the following determines the assignment of data security in this cloud infrastructure?

- ❍ **A.** Playbook
- ❍ **B.** Audit committee
- ❍ **C.** Responsibility matrix
- ❍ **D.** Right-to-audit clause

The Answer: C. Responsibility matrix
A cloud responsibility matrix is usually published by the provider to document the responsibilities for all cloud-based services. For example, the customer responsibilities for an IaaS (Infrastructure as a Service) implementation will be different than SaaS (Software as a Service).

The incorrect answers:
A. Playbook
A playbook provides conditional steps to follow when managing an organization's processes and procedures. For example, the process of recovering from a virus infection would be documented in a playbook.

B. Audit committee
An audit committee oversees the risk management activities for an organization. For example, the committee would be responsible for verifying the security implementation documented in the responsibility matrix.

D. Right-to-audit clause
A right-to-audit clause is often included in a third-party contract to define the terms and conditions around periodic audits. This is often part of a larger product or services contract.

More information:
SY0-701, Objective 3.1 - Cloud Infrastructures
https://professormesser.link/701030101

A66. When decommissioning a device, a company documents the type and size of storage drive, the amount of RAM, and any installed adapter cards. Which of the following describes this process?

- ❍ **A.** Destruction
- ❍ **B.** Sanitization
- ❍ **C.** Certification
- ❍ **D.** Enumeration

The Answer: D. Enumeration
Enumeration describes the detailed listing of all parts in a particular device. For a computer, this could include the CPU type, memory, storage drive details, keyboard model, and more.

The incorrect answers:
A. Destruction
Destruction involves physically damaging a device or component to prevent any future use or data access. Although the company may choose to destroy these computers at a later date, this question does not describe the destruction process.

B. Sanitization
Sanitization deletes data from storage media and allows the storage device to be used in the future. For example, a sector-by-sector format would sanitize a hard drive and allow the drive to be installed into another computer without the concern of a data breach.

C. Certification
If a third-party is providing destruction services, they often will certify the work and document which device serial numbers were destroyed as part of their service.

More information:
SY0-701, Objective 4.2 - Asset Management
https://professormesser.link/701040201

A67. An attacker has sent more information than expected in a single API call, and this has allowed the execution of arbitrary code. Which of the following would BEST describe this attack?

- ❍ **A.** Buffer overflow
- ❍ **B.** Replay attack
- ❍ **C.** Cross-site scripting
- ❍ **D.** DDoS

The Answer: A. Buffer overflow
The results of a buffer overflow can cause random results, but sometimes the actions can be repeatable and controlled. In the best possible case for the hacker, a buffer overflow can be manipulated to execute code on the remote device.

The incorrect answers:
B. Replay attack
A replay attack does not require the sending of more information than expected, and often a replay attack consists of normal traffic and expected application input.

C. Cross-site scripting
A cross-site scripting attack allows a third party to take advantage of the trust a browser might have with another website. This question involves an API call and does not appear to reference a browser or third-party website.

D. DDoS
A DDoS (Distributed Denial of Service) renders a service unavailable, and it involves the input of many devices to operate. A DDoS would not require sending more information than expected, and it rarely results in the execution of arbitrary code.

More information:
SY0-701, Objective 2.3 - Buffer Overflows
https://professormesser.link/701020302

A68. A company encourages users to encrypt all of their confidential materials on a central server. The organization would like to enable key escrow as a backup option. Which of these keys should the organization place into escrow?

- ❍ **A.** Private
- ❍ **B.** CA
- ❍ **C.** Session
- ❍ **D.** Public

The Answer: A. Private
With asymmetric encryption, the private key is used to decrypt information that has been encrypted with the public key. To ensure continued access to the encrypted data, the company must have a copy of each private key.

The incorrect answers:
B. CA
A CA (Certificate Authority) key is commonly used to validate the digital signature from a trusted CA. This is not commonly used for user data encryption.

C. Session
Session keys are commonly used temporarily to provide confidentiality during a single session. Once the session is complete, the keys are discarded. Session keys are not used to provide long-term data encryption.

D. Public
In asymmetric encryption, a public key is already available to everyone. It would not be necessary to escrow a public key.

More information:
SY0-701, Objective 1.4 - Public Key Infrastructure
https://professormesser.link/701010401

A69. A company is in the process of configuring and enabling host-based firewalls on all user devices. Which of the following threats is the company addressing?

- ❍ **A.** Default credentials
- ❍ **B.** Vishing
- ❍ **C.** Instant messaging
- ❍ **D.** On-path

The Answer: C. Instant messaging
Instant messaging is commonly used as an attack vector, and one way to help protect against malicious links delivered by instant messaging is a host-based firewall.

The incorrect answers:
A. Default credentials
Users commonly login with unique credentials that are specific to the user. A host-based firewall would not identify the use of a default username and password.

B. Vishing
Vishing, or voice phishing, occurs over a phone or other voice communication method. A host-based firewall would not be able to protect against a voice-related attack vector.

D. On-path
A on-path attack describes a third-party in the middle of a communications path. The victims of an on-path attack are usually not aware an attack is taking place, so a host-based firewall would not be able to detect an on-path attack.

More information:
SY0-701, Objective 2.2 - Common Threat Vectors
https://professormesser.link/701020201

A70. A manufacturing company would like to use an existing router to separate a corporate network from a manufacturing floor. Both networks use the same physical switch, and the company does not want to install any additional hardware. Which of the following would be the BEST choice for this segmentation?

- ❍ **A.** Connect the corporate network and the manufacturing floor with a VPN
- ❍ **B.** Build an air gapped manufacturing floor network
- ❍ **C.** Use host-based firewalls on each device
- ❍ **D.** Create separate VLANs for the corporate network and the manufacturing floor

.....

The Answer: D. Create separate VLANs for the corporate network and the manufacturing floor

Creating VLANs (Virtual Local Area Networks) will segment a network without requiring additional switches.

The incorrect answers:

A. Connect the corporate network and the manufacturing floor with a VPN

A VPN (Virtual Private Network) would encrypt all information between the two networks, but it would not provide any segmentation. This process would also commonly require additional hardware to provide VPN connectivity.

B. Build an air gapped manufacturing floor network

An air gapped network would require separate physical switches on each side of the gap, and this would require the purchase of an additional switch.

C. Use host-based firewalls on each device

While personal firewalls provide protection for individual devices, they do not segment networks. It's also uncommon for personal firewalls to be installed on manufacturing equipment.

More information:
SY0-701, Objective 2.5 - Segmentation and Access Control
https://professormesser.link/701020501

A71. An organization needs to provide a remote access solution for a newly deployed cloud-based application. This application is designed to be used by mobile field service technicians. Which of the following would be the best option for this requirement?

- ❍ **A.** RTOS
- ❍ **B.** CRL
- ❍ **C.** Zero-trust
- ❍ **D.** SASE

The Answer: D. SASE
A SASE (Secure Access Service Edge) solution is a next-generation VPN technology designed to optimize the process of secure communication to cloud services.

The incorrect answers:
A. RTOS
An RTOS (Real-time Operating System) is an OS designed for industrial equipment, automobiles, and other time-sensitive applications.

B. CRL
A CRL (Certificate Revocation List) is used to determine if a certificate has been administratively revoked. A CRL would not provide any remote access functionality.

C. Zero-trust
Zero-trust is a security strategy where all devices on the network are verified before connecting to another device. Zero-trust does not provide remote access functions.

More information:
SY0-701, Objective 3.2 - Secure Communication
https://professormesser.link/701030207

A72. A company is implementing a quarterly security awareness campaign. Which of the following would MOST likely be part of this campaign?

- ❍ **A.** Suspicious message reports from users
- ❍ **B.** An itemized statement of work
- ❍ **C.** An IaC configuration file
- ❍ **D.** An acceptable use policy document

.....

The Answer: A. Suspicious message reports from users
A security awareness campaign often involves automated phishing attempts, and most campaigns will include a process for users to report a suspected phishing attempt to the IT security team.

The incorrect answers:
B. An itemized statement of work
A statement of work (SOW) is commonly used for service engagements. The SOW provides a list of deliverables for the professional services, and this list is often used to determine if the services were completed.

C. An IaC configuration file
An IaC (Infrastructure as Code) configuration file describes an infrastructure configuration commonly used by cloud-based systems. An IaC configuration file would not be used by a security awareness campaign.

D. An acceptable use policy document
An acceptable use policy (AUP) is defined by an employer to describe the proper use of technology and systems within an organization. The AUP itself is not part of a security awareness campaign.

More information:
SY0-701, Objective 5.6 - Security Awareness
https://professormesser.link/701050601

A73. A recent report shows the return of a vulnerability that was previously patched four months ago. After researching this issue, the security team has found a recent patch has reintroduced this vulnerability on the servers. Which of the following should the security administrator implement to prevent this issue from occurring in the future?

- ❍ **A.** Containerization
- ❍ **B.** Data masking
- ❍ **C.** 802.1X
- ❍ **D.** Change management

The Answer: D. Change management
The change management process includes a testing phase that can help identify potential issues relating to an application change or upgrade.

The incorrect answers:
A. Containerization
Containerization is an efficient method of deploying application instances, but it doesn't provide any mitigation for security vulnerabilities.

B. Data masking
Data masking can be used to limit access to sensitive data, but it does not prevent the implementation of a security vulnerability.

C. 802.1X
802.1X is a standard for port-based network access control, and it can help manage the authentication process of network users. 802.1X does not provide any mitigation for security vulnerabilities.

More information:
SY0-701, Objective 1.3 - Change Management Process
https://professormesser.link/701010301

A74. A security manager would like to ensure that unique hashes are used with an application login process. Which of the following would be the BEST way to add random data when generating a set of stored password hashes?

- ❍ **A.** Salting
- ❍ **B.** Obfuscation
- ❍ **C.** Key stretching
- ❍ **D.** Digital signature

.....

The Answer: A. Salting
Adding random data, or salt, to a password when performing the hashing process will create a unique hash, even if other users have chosen the same password.

The incorrect answers:
B. Obfuscation
Obfuscation is the process of making something difficult for humans to read or understand. The obfuscation process isn't commonly associated with adding random information to hashes.

C. Key stretching
Key stretching uses a cryptographic key multiple times for additional protection against brute force attacks. Key stretching by itself does not commonly add random data to the hashing process.

D. Digital signature
Digital signatures use a hash and asymmetric encryption to provide integrity of data. Digital signatures aren't commonly used for storing passwords.

More information:
SY0-701, Objective 1.4 - Hashing and Digital Signatures
https://professormesser.link/701010406

A75. Which cryptographic method is used to add trust to a digital certificate?

- ❍ **A.** Steganography
- ❍ **B.** Hash
- ❍ **C.** Symmetric encryption
- ❍ **D.** Digital signature

The Answer: D. Digital signature
A certificate authority will digitally sign a certificate to add trust. If you trust the certificate authority, you can therefore trust the certificate.

The incorrect answers:
A. Steganography
Steganography is a technique for hiding information inside of another media type. Steganography is a method of obfuscating data and does not provide a method of adding trust to a certificate.

B. Hash
A hash can help verify that the certificate has not been altered, but it does not provide additional third-party trust.

C. Symmetric encryption
Symmetric encryption provides data confidentiality, but it doesn't add any additional trust to the encryption process.

More information:
SY0-701, Objective 1.4 - Hashing and Digital Signatures
https://professormesser.link/701010406

A76. A company is using SCAP as part of their security monitoring processes. Which of the following would BEST describe this implementation?

- ❍ **A.** Train the user community to better identify phishing attempts
- ❍ **B.** Present the results of an internal audit to the board
- ❍ **C.** Automate the validation and patching of security issues
- ❍ **D.** Identify and document authorized data center visitors

The Answer: C. Automate the validation and patching of security issues
SCAP (Security Content Automation Protocol) focuses on the standardization of vulnerability management across multiple security tools. This allows different tools to identify and act on the same security criteria.

The incorrect answers:
A. Train the user community to better identify phishing attempts
Security awareness training is an important part of an overall security strategy, but the training process does not generally involve SCAP.

B. Present the results of an internal audit to the board
A presentation of audit results can provide important feedback, but the presentation itself does not generally use SCAP.

D. Identify and document authorized data center visitors
The identification and documentation process for visitors is an important security policy, but it does not generally require the use of SCAP.

More information:
SY0-701, Objective 4.4 - Security Tools
https://professormesser.link/701040402

A77. An organization maintains a large database of customer information for sales tracking and customer support. Which person in the organization would be responsible for managing the access rights to this data?

- ❍ **A.** Data processor
- ❍ **B.** Data owner
- ❍ **C.** Data subject
- ❍ **D.** Data custodian

The Answer: D. Data custodian
The data custodian manages access rights and sets security controls to the data.

The incorrect answers:
A. Data processor
The data processor manages the operational use of the data, but not the rights and permissions to the information.

B. Data owner
The data owner is usually a higher-level executive who makes business decisions regarding the data.

C. Data subject
The data subjects are the individuals who have their personal information contained in this customer information database.

More information:
SY0-701, Objective 5.1 - Data Roles and Responsibilities
https://professormesser.link/701050105

A78. An organization's content management system currently labels files and documents as "Public" and "Restricted." On a recent update, a new classification type of "Private" was added. Which of the following would be the MOST likely reason for this addition?

❍ **A.** Minimized attack surface

❍ **B.** Simplified categorization

❍ **C.** Expanded privacy compliance

❍ **D.** Decreased search time

The Answer: C. Expanded privacy compliance
The labeling of data as private is often associated with compliance and confidentiality concerns.

The incorrect answers:
A. Minimized attack surface
The categorization of data has little impact on the size of the potential attack surface associated with a system.

B. Simplified categorization
Adding additional categories would not commonly be considered a simplification.

D. Decreased search time
Adding additional classifications would not necessarily provide any decreased search times.

More information:
SY0-701, Objective 3.3 - Data Types and Classifications
https://professormesser.link/701030301

A79. A corporate security team would like to consolidate and protect the private keys across all of their web servers. Which of these would be the BEST way to securely store these keys?

- ❍ **A.** Integrate an HSM
- ❍ **B.** Implement full disk encryption on the web servers
- ❍ **C.** Use a TPM
- ❍ **D.** Upgrade the web servers to use a UEFI BIOS

The Answer: A. Integrate an HSM
An HSM (Hardware Security Module) is a high-end cryptographic hardware appliance that can securely store keys and certificates for all devices.

The incorrect answers:
B. Implement full disk encryption on the web servers
Full-disk encryption would only protect the keys if someone does not have the proper credentials, and it won't help consolidate all of the web server keys to a central point.

C. Use a TPM
A TPM (Trusted Platform Module) is used on individual devices to provide cryptographic functions and securely store encryption keys. Individual TPMs would not provide any consolidation of web server private keys.

D. Upgrade the web servers to use a UEFI BIOS
A UEFI (Unified Extensible Firmware Interface) BIOS (Basic Input/Output System) does not provide any additional security or consolidation features for web server private keys.

More information:
SY0-701, Objective 1.4 - Encryption Technologies
https://professormesser.link/701010404

A80. A security technician is reviewing this security log from an IPS:

```
ALERT 2023-06-01 13:07:29 [163bcf65118-179b547b]
Cross-Site Scripting in JSON Data
222.43.112.74:3332 -> 64.235.145.35:80
URL/index.html - Method POST - Query String "-"
User Agent: curl/7.21.3 (i386-redhat-linux-gnu) libcurl/7.21.3
NSS/3.13.1.0 zlib/1.2.5 libidn/1.19 libssh2/1.2.7
Detail: token="<script>" key="key7" value="<script>alert(2)</script>"
```

Which of the following can be determined from this log information? (Select TWO)

- ❍ **A.** The alert was generated from a malformed User Agent header
- ❍ **B.** The alert was generated from an embedded script
- ❍ **C.** The attacker's IP address is 222.43.112.74
- ❍ **D.** The attacker's IP address is 64.235.145.35
- ❍ **E.** The alert was generated due to an invalid client port number

The Answer: B. The alert was generated from an embedded script and **C.** The attacker's IP address is 222.43.112.74

The details of the IPS (Intrusion Prevention System) alert show a script value embedded into JSON (JavaScript Object Notation) data. The IPS log also shows the flow of the attack with an arrow in the middle. The attacker was IP address 222.43.112.74 with port 3332, and the victim was 64.235.145.35 over port 80.

The incorrect answers:

A. The alert was generated from a malformed User Agent header
The user agent information is provided as additional supporting data associated with the alert. The agent itself is not the cause of this alert.

D. The attacker's IP address is 64.235.145.35
The attacker's IP address is listed first, so the victim's IP address is 64.235.145.35.

E. The alert was generated due to an invalid client port number
The port number associated with the client, 3332, is a valid port number and not associated with the cause of the alert.

More information:
SY0-701, Objective 4.9 - Log Data
https://professormesser.link/701040901

A81. Which of the following describes a monetary loss if one event occurs?

- ❍ **A.** ALE
- ❍ **B.** SLE
- ❍ **C.** RTO
- ❍ **D.** ARO

The Answer: B. SLE
SLE (Single Loss Expectancy) describes the financial impact of a single event.

The incorrect answers:
A. ALE
ALE (Annual Loss Expectancy) is the financial loss over an entire 12-month period.

C. RTO
RTO (Recovery Time Objectives) define a timeframe needed to restore a particular service level.

D. ARO
The ARO (Annualized Rate of Occurrence) is the number of times an event will occur in a 12-month period.

More information:
SY0-701, Objective 5.2 - Risk Analysis
https://professormesser.link/701050202

A82. A user with restricted access has typed this text in a search field of an internal web-based application:

```
USER77' OR '1'='1
```

After submitting this search request, all database records are displayed on the screen. Which of the following would BEST describe this search?

❍ **A.** Cross-site scripting

❍ **B.** Buffer overflow

❍ **C.** SQL injection

❍ **D.** SSL stripping

The Answer: C. SQL injection
SQL (Structured Query Language) injection takes advantage of poor input validation to circumvent the application and allows the attacker to query the database directly.

The incorrect answers:
A. Cross-site scripting
Cross-site scripting takes advantage of a third-party trust to a web application. The attack demonstrated in this question does not use another user's credentials or access rights to obtain information.

B. Buffer overflow
A buffer overflow uses an application vulnerability to submit more information than an application can properly manage. The attack syntax in this question is specific to SQL injections, and it does not appear to be manipulating a buffer overflow vulnerability.

D. SSL stripping
SSL stripping is a downgrade attack that modifies web site addresses to allow access to encrypted information. The attack in this question does not appear to include a third-party.

More information:
SY0-701, Objective 2.3 - SQL Injection
https://professormesser.link/701020306

A83. A user has opened a helpdesk ticket complaining of poor system performance, excessive pop up messages, and the cursor moving without anyone touching the mouse. This issue began after they opened a spreadsheet from a vendor containing part numbers and pricing information. Which of the following is MOST likely the cause of this user's issues?

❍ **A.** On-path

❍ **B.** Worm

❍ **C.** Trojan horse

❍ **D.** Logic bomb

The Answer: C. Trojan horse
Since a Trojan horse is usually disguised as legitimate software, the victim often doesn't realize they're installing malware. Once the Trojan is installed, the attacker can install additional software to control the infected system.

The incorrect answers:
A. On-path
An on-path attack commonly occurs without any knowledge to the parties involved, and there's usually no additional notification that an attack is underway.

B. Worm
A worm is malware that can replicate itself between systems without any user intervention, so a spreadsheet that requires additional a user to click warning messages would not be categorized as a worm.

D. Logic bomb
A logic bomb is malware that installs and operates silently until a certain event occurs. Once the logic bomb has been triggered, the results usually involve loss of data or a disabled operating system.

More information:
SY0-701, Objective 1.2 - An Overview of Malware
https://professormesser.link/701020401

A84. A web-based manufacturing company processes monthly charges to credit card information saved in the customer's profile. All of the customer information is encrypted and protected with additional authentication factors. Which of the following would be the justification for these security controls?

- ❍ **A.** Chain of custody
- ❍ **B.** Password vaulting
- ❍ **C.** Compliance reporting
- ❍ **D.** Sandboxing

The Answer: C. Compliance reporting
The storage of sensitive information such as customer details and payment information may require additional reporting to ensure compliance with the proper security controls.

The incorrect answers:
A. Chain of custody
Chain of custody describes the control and integrity of collected evidence. Chain of custody would not involve the implementation of encryption and authentication factors in this example.

B. Password vaulting
Password vaults are used as secure storage and retrieval of authentication credentials. The protection of user data is not associated with password vaulting.

D. Sandboxing
Sandboxing is the process of running a service or system in a protected environment. This sandbox allows for testing and analysis without affecting other systems that may currently be in production.

More information:
SY0-701, Objective 5.4 - Compliance
https://professormesser.link/701050401

A85. A security manager has created a report showing intermittent network communication from certain workstations on the internal network to one external IP address. These traffic patterns occur at random times during the day. Which of the following would be the MOST likely reason for these traffic patterns?

- ❍ **A.** On-path attack
- ❍ **B.** Keylogger
- ❍ **C.** Replay attack
- ❍ **D.** Brute force

The Answer: B. Keylogger
A keylogger captures keystrokes and occasionally transmits this information to the attacker for analysis. The traffic patterns identified by the security manager could potentially be categorized as malicious keylogger transfers.

The incorrect answers:
A. On-path attack
An on-path attack is an exploit often associated with a device monitoring data in the middle of a conversation. This question did not provide any evidence of third-party monitoring.

C. Replay attack
A replay attack is often used by an attacker to gain access to a service through the use of credentials gathered from a previous authentication. Internal devices communicating to an external server would not be a common pattern for a replay attack.

D. Brute force
A brute force attack attempts to find authentication credentials by attempting to guess a password. In this example, the source of the traffic and the traffic patterns don't match those seen with common brute force attempts.

More information:
SY0-701, Objective 2.4 - Other Malware Types
https://professormesser.link/701020404

A86. The security policies in a manufacturing company prohibit the transmission of customer information. However, a security administrator has received an alert that credit card numbers were transmitted as an email attachment. Which of the following was the MOST likely source of this alert message?

❍ **A.** IPS

❍ **B.** DLP

❍ **C.** RADIUS

❍ **D.** IPsec

The Answer: B. DLP
DLP (Data Loss Prevention) technologies can identify and block the transmission of sensitive data across the network.

The incorrect answers:
A. IPS
IPS (Intrusion Prevention System) signatures are useful for identifying known vulnerabilities, but they don't commonly provide a way to identify and block PII (Personally Identifiable Information) or sensitive data.

C. RADIUS
RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol commonly used to validate user credentials. RADIUS would not be used to identify sensitive data transfers.

D. IPsec
IPsec (Internet Protocol Security) is a protocol suite for authenticating and encrypting network communication. IPsec does not include any features for identifying and alerting on sensitive information.

More information:
SY0-701, Objective 4.4 - Security Tools
https://professormesser.link/701040402

A87. A security administrator has configured a virtual machine in a screened subnet with a guest login account and no password. Which of the following would be the MOST likely reason for this configuration?

- ❍ **A.** The server is a honeypot for attracting potential attackers
- ❍ **B**. The server is a cloud storage service for remote users
- ❍ **C.** The server will be used as a VPN concentrator
- ❍ **D.** The server is a development sandbox for third-party programming projects

.....

The Answer: A. The server is a honeypot for attracting potential attackers
A screened subnet is a good location to configure services that can be accessed from the Internet, and building a system that can be easily compromised is a common tactic for honeypot systems.

The incorrect answers:
B. The server is a cloud storage service for remote users
Although cloud storage is a useful service, configuring storage on a server with an open guest account is not a best practice.

C. The server will be used as a VPN concentrator
VPN (Virtual Private Networking) concentrators should be installed on secure devices, and configuring an open guest account would not be considered a secure configuration.

D. The server is a development sandbox for third-party programming projects
It would not be secure to configure a development sandbox on a system with an open guest account.

More information:
SY0-701, Objective 1.2 - Deception and Disruption
https://professormesser.link/701010207

A88. A security administrator is configuring a DNS server with a SPF record. Which of the following would be the reason for this configuration?

- ❍ **A.** Transmit all outgoing email over an encrypted tunnel
- ❍ **B.** List all servers authorized to send emails
- ❍ **C.** Digitally sign all outgoing email messages
- ❍ **D.** Obtain disposition instructions for emails marked as spam

.....

The Answer: B. List all servers authorized to send emails
SPF (Sender Policy Framework) is used to publish a list of all authorized email servers for a specific domain.

The incorrect answers:
A. Transmit all outgoing email over an encrypted tunnel
The option to use encrypted protocols for email transfer is configured in the email server and not in the DNS (Domain Name System) server.

C. Digitally sign all outgoing email messages
DKIM (Domain Keys Identified Mail) is used to publish the public key used for the digital signature for all outgoing email.

D. Obtain disposition instructions for emails marked as spam
A DMARC (Domain-based Message Authentication, Reporting, and Conformance) record announces the preferred email disposition if a message is identified as spam. DMARC options include accepting the messages, sending them to a spam folder, or simply rejecting the emails.

More information:
SY0-701, Objective 4.5 - Email Security
https://professormesser.link/701040505

A89. A company would like to securely deploy applications without the overhead of installing a virtual machine for each system. Which of the following would be the BEST way to deploy these applications?

- ❍ **A.** Containerization
- ❍ **B.** IoT
- ❍ **C.** Proxy
- ❍ **D.** RTOS

The Answer: A. Containerization
Application containerization uses a single virtual machine to use as a foundation for separate application "containers." These containers are implemented as isolated instances, and an application in one container is not inherently accessible from other containers on the system.

The incorrect answers:
B. IoT
IoT (Internet of Things) is a broad category of embedded devices often installed in our homes and businesses. IoT devices are not commonly associated with the application deployment process.

C. Proxy
Proxies can be used as security devices, but they aren't commonly used for deploying application instances.

D. RTOS
RTOS (Real-Time Operating Systems) are designed for time-sensitive applications and services. Manufacturing equipment and transportation systems often incorporate an RTOS.

More information:
SY0-701, Objective 3.1 - Other Infrastructure Concepts
https://professormesser.link/701030103

A90. A company has just purchased a new application server, and the security director wants to determine if the system is secure. The system is currently installed in a test environment and will not be available to users until the roll out to production next week. Which of the following would be the BEST way to determine if any part of the system can be exploited?

- ❍ **A.** Tabletop exercise
- ❍ **B.** Vulnerability scanner
- ❍ **C.** DDoS
- ❍ **D.** Penetration test

The Answer: D. Penetration test
A penetration test can be used to actively exploit potential vulnerabilities in a system or application. This could cause a denial of service or loss of data, so the best practice is to perform the penetration test during non-production hours or in a test environment.

The incorrect answers:
A. Tabletop exercise
A tabletop exercise is used to talk through a security event with an incident response team around a conference room table. This is commonly performed as a training device instead of performing a full-scale disaster drill.

B. Vulnerability scanner
Vulnerability scanners may identify a vulnerability, but they do not actively attempt to exploit the vulnerability.

C. DDoS
A DDoS (Distributed Denial of Service) attack is often used to disable a service or application, but it doesn't provide any particular information regarding an application vulnerability.

More information:
SY0-701, Objective 4.3 - Penetration Testing
https://professormesser.link/701040303

B6. A security administrator has performed an audit of the organization's production web servers, and the results have identified default configurations, web services running from a privileged account, and inconsistencies with SSL certificates. Which of the following would be the BEST way to resolve these issues?

- ❍ **A.** Server hardening
- ❍ **B.** Multi-factor authentication
- ❍ **C.** Enable HTTPS
- ❍ **D.** Run operating system updates

The Answer: A. Server hardening
Many applications and services include secure configuration guides to assist in hardening the system. These hardening steps will make the system as secure as possible while simultaneously allowing the application to run efficiently.

The incorrect answers:
B. Multi-factor authentication
Although multi-factor authentication is always a good best practice, simply enabling multiple authentication methods would not resolve the issues identified during the audit.

C. Enable HTTPS
Most web servers will use HTTPS to ensure that network communication is encrypted. However, requiring encrypted network traffic would not correct the issues identified during the audit.

D. Run operating system updates
Keeping the system updated is another good best practice, but the issues identified during the audit were not related to OS patches. Many of the issues identified in the audit appear to be related to the configuration of the web server, so any resolution should focus on correcting these configuration issues.

More information:
SY0-701, Objective 2.5 - Hardening Techniques
https://professormesser.link/701020503

B7. A shipping company stores information in small regional warehouses around the country. The company maintains an IPS at each warehouse to watch for suspicious traffic patterns. Which of the following would BEST describe the security control used at the warehouse?

- ❍ **A.** Deterrent
- ❍ **B.** Compensating
- ❍ **C.** Directive
- ❍ **D.** Detective

The Answer: D. Detective
An IPS can detect, alert, and log an intrusion attempt. The IPS could also be categorized as a preventive control, since it has the ability to actively block known attacks.

The incorrect answers:
A. Deterrent
A deterrent discourages an intrusion attempt, but it doesn't directly prevent the access. An application splash screen or posted warning sign would be categorized as a deterrent.

B. Compensating
A compensating control can't prevent an attack, but it can provide an alternative when an attack occurs. For example, a compensating control would include the re-imaging of a compromised server.

C. Directive
Directive control types are guidelines offered to help direct a subject towards security compliance. Training users on the proper storage of sensitive files would be an example of a directive control.

More information:
SY0-701, Objective 1.1 - Security Controls
https://professormesser.link/701010101

B8. The Vice President of Sales has asked the IT team to create daily backups of the sales data. The Vice President is an example of a:

- ❍ **A.** Data owner
- ❍ **B.** Data controller
- ❍ **C.** Data steward
- ❍ **D.** Data processor

The Answer: A. Data owner
The data owner is accountable for specific data, so this person is often a senior officer of the organization.

The incorrect answers:
B. Data controller
A data controller manages the processing of the data. For example, a payroll department would be a data controller, and a payroll servicing company would be the data processor.

C. Data steward
The data steward manages access rights to the data. In this example, the IT team would be the data steward.

D. Data processor
The data processor is often a third-party that processes data on behalf of the data controller.

More information:
SY0-701, Objective 5.1 - Data Roles and Responsibilities
https://professormesser.link/701050105

B9. A security engineer is preparing to conduct a penetration test of a third-party website. Part of the preparation involves reading through social media posts for information about this site. Which of the following describes this practice?

- ❍ **A.** Partially known environment
- ❍ **B.** OSINT
- ❍ **C.** Exfiltration
- ❍ **D.** Active reconnaissance

The Answer: B. OSINT
OSINT (Open Source Intelligence) describes the process of obtaining information from open sources such as social media sites, corporate websites, online forums, and other publicly available locations.

The incorrect answers:
A. Partially known environment
A partially known environment describes how aware an attacker might be about a test. The attacker may have access to some information about the test, but not all information is disclosed.

C. Exfiltration
Exfiltration describes the theft of data by an attacker.

D. Active reconnaissance
Active reconnaissance would show some evidence of data gathering. For example, performing a ping scan or DNS query wouldn't exploit a vulnerability, but it would show that someone was gathering information.

More information:
SY0-701, Objective 4.3 - Threat Intelligence
https://professormesser.link/701040302

B10. A company would like to orchestrate the response when a virus is detected on company devices. Which of the following would be the BEST way to implement this function?

- ❍ **A.** Active reconnaissance
- ❍ **B.** Log aggregation
- ❍ **C.** Vulnerability scan
- ❍ **D.** Escalation scripting

.....

The Answer: D. Escalation scripting
Scripting and automation can provide methods to automate or orchestrate the escalation response when a security issue is detected.

The incorrect answers:
A. Active reconnaissance
Active reconnaissance will gather information about a system, but it does not provide any ongoing monitoring or response features.

B. Log aggregation
Log aggregation provides a method of centralizing evidence and log files for reporting and future analysis. The aggregated log does not inherently provide a response to a security event.

C. Vulnerability scan
A vulnerability scan will identify any known vulnerabilities that may be associated with a system. However, a vulnerability scan will not identify real-time infections or automate the response.

More information:
SY0-701, Objective 4.7 - Scripting and Automation
https://professormesser.link/701040701

B11. A user in the accounting department has received a text message from the CEO. The message requests payment by cryptocurrency for a recently purchased tablet. Which of the following would BEST describe this attack?

- ❍ **A.** Brand impersonation
- ❍ **B.** Watering hole attack
- ❍ **C.** Smishing
- ❍ **D.** Typosquatting

.....

The Answer: C. Smishing
Smishing is phishing using SMS (Short Message Service), and is more commonly referenced as text messaging. A message allegedly from the CEO asking for an unusual payments using cryptocurrency or gift cards would be categorized as smishing.

The incorrect answers:
A. Brand impersonation
Brand impersonation usually involves a third-party pretending to be an employee or representative of another (usually well-known) company. This text message did not claim a particular brand or trademark as part of the attack.

B. Watering hole attack
A watering hole attack requires users to visit a central website or location. Viewing this text message did not require the user to visit any third-party websites.

D. Typosquatting
A typosquatting attack commonly uses a misspelling of a domain name to redirect victims to a malicious website.

More information:
SY0-701, Objective 2.1 - Phishing
https://professormesser.link/701020202

B12. A company has been informed of a hypervisor vulnerability that could allow users on one virtual machine to access resources on another virtual machine. Which of the following would BEST describe this vulnerability?

- ❍ **A.** Containerization
- ❍ **B.** Jailbreaking
- ❍ **C.** SDN
- ❍ **D.** Escape

.....

The Answer: D. Escape
A VM (Virtual Machine) escape is a vulnerability that allows communication between separate VMs.

The incorrect answers:
A. Containerization
Containerization is an application deployment architecture that uses a self-contained group of application code and dependencies. Using containerization, many separate containers can be deployed simultaneously on a single system.

B. Jailbreaking
Jailbreaking describes the replacement of firmware on a mobile phone or tablet with the goal of enabling or allowing features that would not normally be available. For example, a jailbroken phone or tablet can install software from locations other than the primary app store.

C. SDN
SDN (Software-Defined Networking) separates the control plane of devices from the data plane. This allows for more automation and dynamic changes to the infrastructure.

More information:
SY0-701, Objective 2.3 - Virtualization Vulnerabilities
https://professormesser.link/701020309

B13. While working from home, users are attending a project meeting over a web conference. When typing in the meeting link, the browser is unexpectedly directed to a different website than the web conference. Users in the office do not have any issues accessing the conference site. Which of the following would be the MOST likely reason for this issue?

- ❍ **A.** Buffer overflow
- ❍ **B.** Wireless disassociation
- ❍ **C.** Amplified DDoS
- ❍ **D.** DNS poisoning

The Answer: D. DNS poisoning
An attacker with access to a DNS (Domain Name System) server can modify the DNS configuration files and redirect users to a different website. Anyone using a different DNS server may not see any problems with connectivity to the original site.

The incorrect answers:
A. Buffer overflow
A buffer overflow vulnerability is associated with application input that exceeds the expected input size. A buffer overflow would cause an application to fail or perform unusually, but a buffer overflow would not appear as a redirected web server from a DNS lookup.

B. Wireless deauthentication
Wireless deauthentication would cause users on a wireless network to constantly disconnect. Wireless deauthentication would not cause a redirection of a website.

C. Amplified DDoS
An amplified DDOS (Distributed Denial of Service) would attack a service from many different devices and cause the service to be unavailable. This attack sends specially crafted packets to maximize the amount of traffic seen in the response. In this example, the service did not document any availability problems.

More information:
SY0-701, Objective 2.4 - DNS Attacks
https://professormesser.link/701020407

B14. A company is launching a new internal application that will not start until a username and password is entered and a smart card is plugged into the computer. Which of the following BEST describes this process?

- ❍ **A.** Federation
- ❍ **B.** Accounting
- ❍ **C.** Authentication
- ❍ **D.** Authorization

.....

The Answer: C. Authentication
The process of proving who you say you are is authentication. In this example, the password and smart card are two factors of authentication, and both reasonably prove that the person with the login credentials is authentic.

The incorrect answers:
A. Federation
Federation provides a way to authenticate and authorize between two different organizations. In this example, the authentication process uses internal information without any type of connection or trust to a third-party.

B. Accounting
Accounting will document information regarding a user's session, such as login time, data sent and received, files transferred, and logout time.

D. Authorization
The authorization process assigns users to resources. This process commonly occurs after the authentication process is complete.

More information:
SY0-701, Objective 1.2
Authentication, Authorization, and Accounting
https://professormesser.link/701010203

B15. An online retailer is planning a penetration test as part of their PCI DSS validation. A third-party organization will be performing the test, and the online retailer has provided the Internet-facing IP addresses for their public web servers. No other details were provided. What penetration testing methodology is the online retailer using?

- ❍ **A.** Known environment
- ❍ **B.** Passive reconnaissance
- ❍ **C.** Partially known environment
- ❍ **D.** Benchmarks

The Answer: C. Partially known environment
A partially known environment test is performed when the attacker knows some information about the victim, but not all information is available.

The incorrect answers:
A. Known environment
A known environment test is performed when the attacker has complete details about the victim's systems and infrastructure.

B. Passive reconnaissance
Passive reconnaissance is the process of gathering information from publicly available sites, such as social media or corporate websites.

D. Benchmarks
Security benchmarks describe a set of best practices to apply to an application, operating system, or any other service. A benchmark does not describe the information provided to a vulnerability scanning service.

More information:
SY0-701, Objective 5.5 - Penetration Tests
https://professormesser.link/701050502

B16. A manufacturing company produces radar used by commercial and military organizations. A recently proposed policy change would allow the use of mobile devices inside the facility. Which of the following would be the MOST significant threat vector issue associated with this change in policy?

- ❍ **A.** Unauthorized software on rooted devices
- ❍ **B.** Remote access clients on the mobile devices
- ❍ **C.** Out of date mobile operating systems
- ❍ **D.** Loss of intellectual property

.....

The Answer: D. Loss of intellectual property
The exfiltration of confidential information and intellectual property is relatively simple with an easily transportable mobile phone. Organizations associated with sensitive products or services must always be aware of the potential for information leaks using files, photos, or video.

The incorrect answers:
A. Unauthorized software on rooted devices
Although unauthorized software use can be a security issue, it isn't as significant as the exfiltration of intellectual property.

B. Remote access clients on the mobile devices
It's sometimes convenient to have a remote access client available, and this type of access can certainly be a concern if the proper security is not in place. However, the much more significant security issue in this list would be associated with the ease of photos and videography when working with confidential information.

C. Out of date mobile operating systems
Having an outdated operating system can potentially include security vulnerabilities, but these vulnerabilities do not have the significance of an active data exfiltration method.

More information:
SY0-701, Objective 2.2 - Common Threat Vectors
https://professormesser.link/701020201

B17. Which of the following would be the BEST way for an organization to verify the digital signature provided by an external email server?

- ❍ **A.** Perform a vulnerability scan
- ❍ **B.** View the server's device certificate
- ❍ **C.** Authenticate to a RADIUS server
- ❍ **D.** Check the DKIM record

The Answer: D. Check the DKIM record
A DKIM (Domain Keys Identified Mail) record is a DNS (Domain Name System) entry that includes the public key associated with an email server's digital signatures. A legitimate email server will digitally sign all outgoing emails and provide the public key in their DNS for third-party validation.

The incorrect answers:
A. Perform a vulnerability scan
A vulnerability scan can provide information on any unpatched applications or services, but it won't provide digital signature verification for incoming email messages.

B. View the server's device certificate
A device certificate can validate the trust of a system, but it does not provide digital signature validation for email servers.

C. Authenticate to a RADIUS server
A RADIUS server can verify account credentials, but it does not provide a method for validating the digital signatures provided by a third-party email server.

More information:
SY0-701, Objective 4.5 - Email Security
https://professormesser.link/701040505

B18. A company is using older operating systems for their web servers and are concerned of their stability during periods of high use. Which of the following should the company use to maximize the uptime and availability of this service?

- ❍ **A.** Cold site
- ❍ **B.** UPS
- ❍ **C.** Redundant routers
- ❍ **D.** Load balancer

.....

The Answer: D. Load balancer
A load balancer maintains a pool of servers and can distribute the load across those devices. If a device fails, the other servers will continue to operate and provide the necessary services.

The incorrect answers:
A. Cold site
A cold site is commonly used for disaster recovery and would require building an infrastructure and installing software before the site would be functional. Moving the web services to a cold site would not be an efficient form of server resiliency.

B. UPS
A UPS (Uninterruptible Power Supply) provides an alternative power source when the main power is no longer available. Although this would provide additional uptime for power faults, it does not provide resiliency if an operating system crashes.

C. Redundant routers
Maintaining multiple routers is common in highly available networks, but multiple routers will not provide uptime if the server operating system was to fail.

More information:
SY0-701, Objective 3.4 - Resiliency
https://professormesser.link/701030401

B19. A user in the accounting department would like to email a spreadsheet with sensitive information to a list of third-party vendors. Which of the following would be the BEST way to protect the data in this email?

- ❍ **A.** Full disk encryption
- ❍ **B.** Key exchange algorithm
- ❍ **C.** Salted hash
- ❍ **D.** Asymmetric encryption

The Answer: D. Asymmetric encryption
Asymmetric encryption uses a recipient's public key to encrypt data, and this data can only be decrypted with the recipient's private key. This encryption method is commonly used with software such as PGP or GPG.

The incorrect answers:
A. Full disk encryption
Full disk encryption protects all data saved on a storage drive, but it does not provide any data protection for messages or attachments sent between email servers.

B. Key exchange algorithm
A key exchange algorithm can be used to securely exchange key information between devices, but it does not provide a method of encrypting data.

C. Salted hash
A salted hash describes a hash value that includes some additional data (the salt) to provide randomization. A salted hash does not provide data confidentiality or encryption.

More information:
SY0-701, Objective 1.4 - Encrypting Data
https://professormesser.link/701010402

B20. A system administrator would like to segment the network to give the marketing, accounting, and manufacturing departments their own private network. The network communication between departments would be restricted for additional security. Which of the following should be configured on this network?

- ❍ **A.** VPN
- ❍ **B.** RBAC
- ❍ **C.** VLAN
- ❍ **D.** SDN

The Answer: C. VLAN
A VLAN (Virtual Local Area Network) is a common method of using a switch to logically segment a network. The devices in each segmented VLAN can only communicate with other devices in the same VLAN. A router is used to connect VLANs, and this router can often be used to control traffic flows between the VLANs.

The incorrect answers:
A. VPN
A VPN (Virtual Private Network) is an encryption technology used to secure network connections between sites or remote end-user communication. VPNs are not commonly used to segment internal network communication.

B. RBAC
RBAC (Role-Based Access Control) describes a control mechanism for managing rights and permissions in an operating system. RBAC is not used for network segmentation.

D. SDN
SDN (Software Defined Networking) separates the planes of operation so that infrastructure devices would have a defined control plane and data plane. SDN would not be used when segmenting internal networks.

More information:
SY0-701, Objective 2.5 - Segmentation and Access Control
https://professormesser.link/701020501

B21. A technician at an MSP has been asked to manage devices on third-party private network. The technician needs command line access to internal routers, switches, and firewalls. Which of the following would provide the necessary access?

- ❍ **A.** HSM
- ❍ **B.** Jump server
- ❍ **C.** NAC
- ❍ **D.** Air gap

The Answer: B. Jump server
A jump server is a highly secured device commonly used to access secure areas of another network. The technician would first connect to the jump server using SSH or a VPN tunnel, and then "jump" from the jump server to other devices on the inside of the protected network. This would allow technicians at an MSP (Managed Service Provider) to securely access devices on their customer's private networks.

The incorrect answers:
A. HSM
An HSM (Hardware Security Module) is a secure method of cryptographic key backup and hardware-based cryptographic offloading.

C. NAC
NAC (Network Access Control) is a broad term describing access control based on a health check or posture assessment. NAC will deny access to devices that don't meet the minimum security requirements.

D. Air gap
An air gap is a segmentation strategy that separates devices or networks by physically disconnecting them from each other.

More information:
SY0-701, Objective 3.2 - Network Appliances
https://professormesser.link/701030203

B22. A transportation company is installing new wireless access points in their corporate office. The manufacturer estimates the access points will operate an average of 100,000 hours before a hardware-related outage. Which of the following describes this estimate?

- ❍ **A.** MTTR
- ❍ **B.** RPO
- ❍ **C.** RTO
- ❍ **D.** MTBF

.....

The Answer: D. MTBF
The MTBF (Mean Time Between Failures) is the average time expected between outages. This is usually an estimation based on the internal device components and their expected operational lifetime.

The incorrect answers:
A. MTTR
MTTR (Mean Time to Repair) is the time required to repair a product or system after a failure.

B. RPO
RPO (Recovery Point Objectives) define how much data loss would be acceptable during a recovery.

C. RTO
RTO (Recovery Time Objectives) define the minimum objectives required to get up and running to a particular service level.

More information:
SY0-701, Objective 5.2 - Business Impact Analysis
https://professormesser.link/701050204

B23. A security administrator is creating a policy to prevent the disclosure of credit card numbers in a customer support application. Users of the application would only be able to view the last four digits of a credit card number. Which of the following would provide this functionality?

- ❍ **A.** Hashing
- ❍ **B.** Tokenization
- ❍ **C.** Masking
- ❍ **D.** Salting

The Answer: C. Masking
Data masking hides data from being viewed. The full credit card numbers are stored in a database, but only a limited view of this data is available when accessing the information from the application.

The incorrect answers:
A. Hashing
Hashing is a method of storing a digital fingerprint of data. In this example, the last four digits displayed are the actual card numbers and not a hash of the card numbers.

B. Tokenization
Tokenization replaces sensitive data with a non-sensitive placeholder. In this example, the only visible information is part of the actual card number. Tokenization is not used to replace any of the card numbers.

D. Salting
Salting adds randomized data when performing a hashing function. Salting is often used to add additional randomization when storing passwords.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

B24. A user is authenticating through the use of a PIN and a fingerprint. Which of the following would describe these authentication factors?

- ❍ **A.** Something you know, something you are
- ❍ **B.** Something you are, somewhere you are
- ❍ **C.** Something you have, something you know
- ❍ **D.** Somewhere you are, something you are

The Answer: A. Something you know, something you are
A PIN (Personal Identification Number) is something you know, and a fingerprint is something you are.

The incorrect answers:
B. Something you are, somewhere you are
A fingerprint would be categorized as something you are, but a somewhere you are could be a set of GPS coordinates or IP addresses.

C. Something you have, something you know
Something you have could be an smart ID card or phone app, and something you know could be a PIN or password.

D. Somewhere you are, something you are
Somewhere you are would be a location, and something you are would be a biometric reading.

More information:
SY0-701, Objective 4.6 - Multi-factor Authentication
https://professormesser.link/701040603

B25. A security administrator is configuring the authentication process used by technicians when logging into wireless access points and switches. Instead of using local accounts, the administrator would like to pass all login requests to a centralized database. Which of the following would be the BEST way to implement this requirement?

- ❍ **A.** COPE
- ❍ **B.** AAA
- ❍ **C.** IPsec
- ❍ **D.** SIEM

The Answer: B. AAA
Using AAA (Authentication, Authorization, and Accounting) is a common method of centralizing authentication. Instead of having separate local accounts on different devices, users can authenticate with account information maintained in a centralized database.

The incorrect answers:
A. COPE
COPE (Corporate-owned, personally enabled) devices are purchased by the organization and enabled for both business and personal use. A COPE device does not provide any centralized authentication functionality.

C. IPsec
IPsec is commonly used as an encrypted tunnel between sites or endpoints. It's useful for protecting data sent over the network, but IPsec isn't used to centralize the authentication process.

D. SIEM
A SIEM (Security Information and Event Management) service provides centralized logging and reporting for network infrastructure devices. A SIEM service does not provide any centralized authentication features.

More information:
SY0-701, Objective 4.1 - Wireless Security Settings
https://professormesser.link/701040104

B26. A recent audit has determined that many IT department accounts have been granted Administrator access. The audit recommends replacing these permissions with limited access rights. Which of the following would describe this policy?

- ❍ **A.** Password vaulting
- ❍ **B.** Offboarding
- ❍ **C.** Least privilege
- ❍ **D.** Discretionary access control

.....

The Answer: C. Least privilege
The policy of least privilege limits the rights and permissions of a user account to only the access required to accomplish their objectives. This policy would limit the scope of an attack originating from a user in the IT department.

The incorrect answers:
A. Password vaulting
Password vaulting is a secure way to store and retrieve passwords, but it doesn't include a policy for limiting system access.

B. Offboarding
The offboarding process describes the policies and procedures associated with someone leaving the organization or someone who is no longer an employee of the company.

D. Discretionary access control
With discretionary access control (DAC), access and permissions are determined by the owner or originator of the files or resources.

More information:
SY0-701, Objective 4.6 - Access Controls
https://professormesser.link/701040602

B27. A recent security audit has discovered usernames and passwords which can be easily viewed in a packet capture. Which of the following did the audit identify?

- ❍ **A.** Weak encryption
- ❍ **B.** Improper patch management
- ❍ **C.** Insecure protocols
- ❍ **D.** Open ports

The Answer: C. Insecure protocols
An insecure authentication protocol will transmit information "in the clear," or without any type of encryption or protection.

The incorrect answers:
A. Weak encryption
A weak encryption cipher will appear to protect data, but instead can be commonly circumvented to reveal the plaintext. In this example, the usernames and passwords were not encrypted in any way and could be viewed in a packet capture.

B. Improper patch management
Maintaining systems to the latest patch version will protect against vulnerabilities and security issues. Sending information in the clear over the network is not commonly associated with an unpatched system.

D. Open ports
Open ports are usually associated with a service or application on a device. An open port is not commonly associated with any encryption or protected network communication.

More information:
SY0-701, Objective 4.5 - Secure Protocols
https://professormesser.link/701040504

B28. Before deploying a new application, a company is performing an internal audit to ensure all of their servers are configured with the appropriate security features. Which of the following would BEST describe this process?

- ❍ **A.** Due care
- ❍ **B.** Active reconnaissance
- ❍ **C.** Data retention
- ❍ **D.** Statement of work

.....

The Answer: A. Due care
Due care describes a duty to act honestly and in good faith. Due diligence is often associated with third-party activities, and due care tends to refer to internal activities.

The incorrect answers:
B. Active reconnaissance
Active reconnaissance refers to the process of collecting information before a penetration test. Active reconnaissance includes activities that will communicate to devices where traffic can be logged.

C. Data retention
Data retention involves the collection and storage of data over time. For example, many organizations are required to collect and store years of email records or financial documents.

D. Statement of work
A statement of work is often used during a professional services engagement to detail a list of specific tasks to complete. In this example, all of the work is part of an internal audit and does not include any mention of third-party professional services.

More information:
SY0-701, Objective 5.4 - Compliance
https://professormesser.link/701050401

B29. An organization has previously purchased insurance to cover a ransomware attack, but the costs of maintaining the policy have increased above the acceptable budget. The company has now decided to cancel the insurance policies and address potential ransomware issues internally. Which of the following would best describe this action?

- ❍ **A.** Mitigation
- ❍ **B.** Acceptance
- ❍ **C.** Transference
- ❍ **D.** Risk-avoidance

The Answer: B. Acceptance
Risk acceptance is a business decision that places the responsibility of the risky activity on the organization itself.

The incorrect answers:
A. Mitigation
If the organization was to purchase additional backup facilities and update their backup processes to include offline backup storage, they would be mitigating the risk of a ransomware infection.

C. Transference
Purchasing insurance to cover a risky activity is a common method of transferring risk from the organization to the insurance company.

D. Risk-avoidance
To avoid the risk of ransomware, the organization would need to completely disconnect from the Internet and disable all methods that ransomware might use to infect a system. This risk response technique would most likely not apply to ransomware.

More information:
SY0-701, Objective 5.2 - Risk Management Strategies
https://professormesser.link/701050203

B30. Which of these threat actors would be MOST likely to install a company's internal application on a public cloud provider?

- ❍ **A.** Organized crime
- ❍ **B.** Nation state
- ❍ **C.** Shadow IT
- ❍ **D.** Hacktivist

The Answer: C. Shadow IT
Shadow IT is an internal organization within the company but is not part of the IT department. Shadow IT often circumvents or ignores existing IT policies to build their own infrastructure with company resources.

The incorrect answers:
A. Organized crime
Organized crime is usually motivated by money. An organized crime group is more interested in stealing information than installing company applications in a public cloud.

B. Nation state
Nation states are highly sophisticated hackers, and their efforts are usually focused on obtaining confidential government information or disrupting governmental operations.

D. Hacktivist
A hacktivist often has a political statement to make, and their hacking efforts would commonly result in a public display of that information. However, a hacktivist would not install company application on a public cloud provider's network.

More information:
SY0-701, Objective 2.1 - Threat Actors
https://professormesser.link/701020101

B31. An IPS report shows a series of exploit attempts were made against externally facing web servers. The system administrator of the web servers has identified a number of unusual log entries on each system. Which of the following would be the NEXT step in the incident response process?

- ❍ **A.** Check the IPS logs for any other potential attacks
- ❍ **B.** Create a plan for removing malware from the web servers
- ❍ **C.** Disable any breached user accounts
- ❍ **D.** Disconnect the web servers from the network

.....

The Answer: D. Disconnect the web servers from the network
The unusual log entries on the web server indicate that the system may have been exploited. In that situation, the servers should be contained to prevent all connectivity to those systems.

The incorrect answers:
A. Check the IPS logs for any other potential attacks
Before looking for additional intrusions, the devices showing a potential exploit should be contained.

B. Create a plan for removing malware from the web servers
The eradication and recovery processes should occur after the systems have been isolated and contained.

C. Disable any breached user accounts
Disabling accounts is part of the recovery process, and it should occur after the exploited servers are contained.

More information:
SY0-701, Objective 4.8 - Incident Response
https://professormesser.link/701040801

B32. A security administrator is viewing the logs on a laptop in the shipping and receiving department and identifies these events:

```
8:55:30 AM | D:\Downloads\ChangeLog-5.0.4.scr | Quarantine Success
9:22:54 AM | C:\Program Files\Photo Viewer\ViewerBase.dll | Quarantine Failure
9:44:05 AM | C:\Sales\Sample32.dat | Quarantine Success
```

Which of the following would BEST describe the circumstances surrounding these events?

- ❍ **A.** The antivirus application identified three viruses and quarantined two viruses
- ❍ **B.** The host-based firewall blocked two traffic flows
- ❍ **C.** A host-based allow list has blocked two applications from executing
- ❍ **D.** A network-based IPS has identified two known vulnerabilities

.....

The Answer: A. The antivirus application identified three viruses and quarantined two viruses

The logs are showing the name of files on the local device and a quarantine disposition, which indicates that two of the files were moved (quarantined) to a separate area of the drive. This will prevent the malicious files from executing and will safely store the files for any future investigation. The second file in the list failed the quarantine process, and was most likely because the library was already in use by the operating system and could not be moved.

The incorrect answers:

B. The host-based firewall blocked two traffic flows

A host-based firewall will allow or deny traffic flows based on IP address, port number, application, or other criteria. A host-based firewall does not block traffic flows based on the name of an existing file, and the firewall process would not quarantine or move files to other folders.

C. A host-based allow list has blocked two applications from executing
The "quarantine" disposition refers to a file that has been moved from one location to another. An allow list function would simply stop the application from executing without changing the location of an application file.

D. A network-based IPS has identified two known vulnerabilities
The logs from a network-based IPS (Intrusion Prevention System) would not commonly be located on a user's laptop, and those logs would display allow or deny dispositions based on the name of a known vulnerability. A network-based IPS would also not commonly move (quarantine) files on an end-user's computer.

More information:
SY0-701, Objective 4.9- Log Data
https://professormesser.link/701040901

B33. In the past, an organization has relied on the curated Apple App Store to avoid issues associated with malware and insecure applications. However, the IT department has discovered an iPhone in the shipping department with applications not available on the Apple App Store. How did the shipping department user install these apps on their mobile device?

- ❍ **A.** Side loading
- ❍ **B.** Malicious update
- ❍ **C.** VM escape
- ❍ **D.** Cross-site scripting

.....

The Answer: A. Side loading
If Apple's iOS has been circumvented using jailbreaking, a user can install apps without using the Apple App Store. Circumventing a curated app store to install an app manually is called side loading.

The incorrect answers:
B. Malicious update
A malicious update would patch an existing app and would not commonly install a different app onto a mobile device.

C. VM escape
VM (Virtual Machine) escape describes the unauthorized access of one VM from a different VM on the same hypervisor. An app installation on a phone is not related to virtual machines.

D. Cross-site scripting
Cross-site scripting is an attack that uses the trust in a browser to gain access to a third-party site. The installation of an app isn't commonly associated with cross-site scripting.

More information:
SY0-701, Objective 2.3 - Mobile Device Vulnerabilities
https://professormesser.link/701020313

B34. A company has noticed an increase in support calls from attackers. These attackers are using social engineering to gain unauthorized access to customer data. Which of the following would be the BEST way to prevent these attacks?

- ❍ **A.** User training
- ❍ **B.** Next-generation firewall
- ❍ **C.** Internal audit
- ❍ **D.** Penetration testing

.....

The Answer: A. User training
Many social engineering attacks do not involve technology, so the best way to prevent the attack is to properly train users to watch for these techniques.

The incorrect answers:
B. Next-generation firewall
A next-generation firewall can provide extensive protection against attacks involving technology, but a firewall can't stop a phone conversation or similar type of social engineering.

C. Internal audit
An internal audit may be able to recognize and report on the increase in social engineering attacks, but an audit does not provide a method of stopping the attack from originally occurring.

D. Penetration testing
Penetration testing can identify vulnerabilities and can attempt to exploit those vulnerabilities. Penetration testing does not block an attack from occurring.

More information:
SY0-701, Objective 5.6 - User Training
https://professormesser.link/701050602

B35. As part of an internal audit, each department of a company has been asked to compile a list of all devices, operating systems, and applications in use. Which of the following would BEST describe this audit?

- ❍ **A.** Attestation
- ❍ **B.** Self-assessment
- ❍ **C.** Regulatory compliance
- ❍ **D.** Vendor monitoring

.....

The Answer: B. Self-assessment
A self-assessment describes an organization performing their own security checks.

The incorrect answers:
A. Attestation
Attestation is commonly one of the last steps when performing an audit. This attestation is an opinion of the truth or accuracy of a company's security position.

C. Regulatory compliance
Regulatory compliance is often required to validate a specific security posture. For example, an organization storing credit card information may be required by regulation to ensure the confidentiality of that data. This question does not mention any type of regulation as the reason for this information gathering.

D. Vendor monitoring
When working with a third-party, it's often important to maintain an ongoing audit and monitoring processes with the vendor. In this example, all of the information gathering is with internal company departments.

More information:
SY0-701, Objective 5.5 - Audits and Assessments
https://professormesser.link/701050501

B36. A company is concerned about security issues at their remote sites. Which of the following would provide the IT team with more information of potential shortcomings?

- ❍ **A.** Gap analysis
- ❍ **B.** Policy administrator
- ❍ **C.** Change management
- ❍ **D.** Dependency list

.....

The Answer: A. Gap analysis
A gap analysis is a formal process comparing the current security posture with where the company would like to be. This often examines many different aspects of the overall security environment.

The incorrect answers:
B. Policy administrator
The Policy Administrator is used in a zero-trust environment to generate access tokens or credentials.

C. Change management
The change management process is important for the controlled deployment of system changes, but it doesn't help provide an overview of security shortcomings.

D. Dependency list
A list of dependencies is often used during technical change management to plan for any potential changes. Before a change can occur, all of the dependencies associated with that change must be addressed.

More information:
SY0-701, Objective 1.2 - Gap Analysis
https://professormesser.link/701010204

B37. An attacker has identified a number of devices on a corporate network with the username of "admin" and the password of "admin." Which of the following describes this situation?

- ❍ **A.** Open service ports
- ❍ **B.** Default credentials
- ❍ **C.** Unsupported systems
- ❍ **D.** Phishing

.....

The Answer: B. Default credentials
When a device is first installed, it will often have a default set of credentials such as admin/password or admin/admin. If these default credentials are never changed, they would allow access by anyone who knows the default configuration.

The incorrect answers:
A. Open service ports
Service ports are commonly opened when an inbound connection needs to be made to a service. For example, a web server will open ports 80 and 443 to allow all incoming traffic requests by the service.

C. Unsupported systems
Unsupported systems describe devices or services no longer supported by the manufacturer. An unsupported system may not receive ongoing security patches or updates.

D. Phishing
Phishing uses social engineering to obtain sensitive or private information. A device using the default credentials would not require a phishing attack to determine the valid username and password.

More information:
SY0-701, Objective 2.2 - Common Threat Vectors
https://professormesser.link/701020201

B38. A security administrator attends an annual industry convention with other security professionals from around the world. Which of the following attacks would be MOST likely in this situation?

- ❍ **A.** Smishing
- ❍ **B.** Supply chain
- ❍ **C.** SQL injection
- ❍ **D.** Watering hole

The Answer: D. Watering hole
A watering hole attack infects a third-party visited by the intended victims. An industry convention would be a perfect location to attack security professionals.

The incorrect answers:
A. Smishing
Smishing, or SMS phishing, is a phishing attack over text messaging. A security administrator attending an industry event would not be the best possible scenario for smishing.

B. Supply chain
A supply chain attack infects part of the product manufacturing process in an attempt to also infect everything further down the chain. An industry trade event would not be a common vector for a supply chain attack.

C. SQL injection
A SQL (Structured Query Language) injection attack takes advantage of a software vulnerability to allow direct access to a SQL database. A SQL injection is not commonly directed towards an individual or an event.

More information:
SY0-701, Objective 2.2 - Watering Hole Attacks
https://professormesser.link/701020204

B39. A transportation company headquarters is located in an area with frequent power surges and outages. The security administrator is concerned about the potential for downtime and hardware failures. Which of the following would provide the most protection against these issues? Select TWO.

- ❍ **A.** UPS
- ❍ **B.** Parallel processing
- ❍ **C.** Snapshots
- ❍ **D.** Multi-cloud system
- ❍ **E.** Load balancing
- ❍ **F.** Generator

The Answers: A. UPS and **F.** Generator
A UPS (Uninterruptible Power Supply) can provide backup power for a limited time when the main power source is unavailable, and a generator can maintain uptime as long as a fuel source is available.

The incorrect answers:
B. Parallel processing
Parallel processing uses multiple processors across multiple systems to improve the performance of an application. Parallel processing will not protect against power outages.

C. Snapshots
A snapshot is a type of backup commonly associated with virtual machines (VMs). Taking the snapshot of a VM can provide an easy method of reverting to an earlier configuration, but it doesn't help for power issues.

D. Multi-cloud system
An application hosted across multiple cloud providers would not provide any resiliency for power-related issues in a local data center.

E. Load balancing
Load balancers provide a method of managing busy services by increasing the number of available servers and balancing the load between them. A load balancer won't provide any help with power issues, however.

More information:
SY0-701, Objective 3.4 - Power Resiliency
https://professormesser.link/701030405

B40. An organization has developed an in-house mobile device app for order processing. The developers would like the app to identify revoked server certificates without sending any traffic over the corporate Internet connection. Which of the following must be configured to allow this functionality?

- ❍ **A.** CSR generation
- ❍ **B.** OCSP stapling
- ❍ **C.** Key escrow
- ❍ **D.** Wildcard

The Answer: B. OCSP stapling
The use of OCSP (Online Certificate Status Protocol) requires communication between the client and the issuing CA (Certificate Authority). If the CA is an external organization, then validation checks will communicate across the Internet. The certificate holder can verify their own status and avoid client Internet traffic by storing the status information on an internal server and "stapling" the OCSP status into the SSL/TLS handshake.

The incorrect answers:
A. CSR generation
A CSR (Certificate Signing Request) is used during the key creation process. The certificate is sent to the CA to be signed as part of the CSR.

C. Key escrow
Key escrow will provide a third-party with access to decryption keys. The escrow process is not involved in real-time server revocation updates.

D. Wildcard
A wildcard certificate can be used across many different systems matching the fully qualified domain name associated with the wildcard.

More information:
SY0-701, Objective 1.4 - Certificates
https://professormesser.link/701010408

B41. A security administrator has been asked to build a network link to secure all communication between two remote locations. Which of the following would be the best choice for this task?

- ❍ **A.** SCAP
- ❍ **B.** Screened subnet
- ❍ **C.** IPsec
- ❍ **D.** Network access control

.....

The Answer: C. IPsec
IPsec (Internet Protocol Security) is commonly used to create a VPN (Virtual Private Network) protected tunnel between devices or locations.

The incorrect answers:
A. SCAP
The SCAP (Security Content Automation Protocol) is used as a common protocol across multiple security tools. SCAP is not used to provide an encrypted tunnel between two locations.

B. Screened subnet
A screened subnet is a protected area commonly used to host public services without allowing access to an organization's internal private network.

D. Network access control
Network access control (NAC) describes the authentication and authorization process when devices connect to a network. NAC is not used to connect two sites over an encrypted channel.

More information:
SY0-701, Objective 3.2 - Secure Communication
https://professormesser.link/701030206

B42. A Linux administrator has received a ticket complaining of response issues with a database server. After connecting to the server, the administrator views this information:

```
Filesystem  Size  Used Avail Use% Mounted on
/dev/xvda1  158G  158G     0 100% /
```

Which of the following would BEST describe this information?

❍ **A.** Buffer overflow

❍ **B.** Resource consumption

❍ **C.** SQL injection

❍ **D.** Race condition

The Answer: B. Resource consumption
The available storage on the local filesystem has been depleted, and the information shows 0 bytes available. More drive space would need to be available for the server to return to normal response times.

The incorrect answers:
A. Buffer overflow
A buffer overflow allows an attacker to manipulate the contents of memory. A filesystem at 100% utilization does not describe the contents in memory.

C. SQL injection
A SQL injection is a network attack type used to access database information directly. A SQL injection would not cause significant storage drive utilization.

D. Race condition
A race condition is a programming issue where a portion of the application is making changes not seen by other parts of the application. A race condition does not commonly use all available storage space on the device.

More information:
SY0-701, Objective 2.4 - Indicators of Compromise
https://professormesser.link/701020415

B43. Which of the following can be used for credit card transactions from a mobile device without sending the actual credit card number across the network?

- ❍ **A.** Tokenization
- ❍ **B.** Hashing
- ❍ **C.** Steganography
- ❍ **D.** Masking

.....

The Answer: A. Tokenization
Tokenization replaces sensitive data with a non-sensitive placeholder. Tokenization is commonly used for NFC (Near-Field Communication) payment systems, and sends a single-use token across the network instead of the actual credit card information.

The incorrect answers:
B. Hashing
Hashing creates a digital "fingerprint" of data, but hashing isn't used to transfer card numbers or other financial details from one device to another.

C. Steganography
Steganography describes hiding data within other media types. For example, it's common to use steganography to hide text documents within an image file. However, steganography is not commonly used to transfer credit card transactions across the network.

D. Masking
Data masking hides some of the original data to protect sensitive information. Credit card transfers cannot omit or hide data necessary to complete the transaction.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

B44. A security administrator receives a report each week showing a Linux vulnerability associated with a Windows server. Which of the following would prevent this information from appearing in the report?

- ❍ **A.** Alert tuning
- ❍ **B.** Application benchmarking
- ❍ **C.** SIEM aggregation
- ❍ **D.** Data archiving

The Answer: A. Alert tuning
Our monitoring systems are not always perfect, and many require ongoing tuning to properly configure alerts and notifications of important events.

The incorrect answers:
B. Application benchmarking
Creating an application benchmark can help with the planning and implementation of security monitoring. However, the creation of an application benchmark does not change the alert messages created by a third-party monitoring system.

C. SIEM aggregation
A SIEM (Security Information and Event Manager) can be used to aggregate all log files to a centralized reporting system. Creating a centralized log repository does not remove invalid alerts from a weekly report.

D. Data archiving
Many organizations are required to archive data for long-term security monitoring. Simply archiving the data does not change the alert notification in a weekly report.

More information:
SY0-701, Objective 4.4 - Security Monitoring
https://professormesser.link/701040401

B45. Which of the following would a company use to calculate the loss of a business activity if a vulnerability is exploited?

- ❍ **A.** Risk tolerance
- ❍ **B.** Vulnerability classification
- ❍ **C.** Environmental variables
- ❍ **D.** Exposure factor

.....

The Answer: D. Exposure factor
An exposure factor describes a loss of value to the organization. For example, a network throughput issue might limit access to half of the users, creating a 50% exposure factor. A completely disabled service would calculated as a 100% exposure factor.

The incorrect answers:
A. Risk tolerance
Risk tolerance describes the amount of risk that would be acceptable to an organization. For example, an organization may tolerate the risk involved with a delay so that patches can be tested prior to deployment.

B. Vulnerability classification
Most vulnerabilities are classified into categories and are often assigned a score to designate the severity of the known vulnerability.

C. Environmental variables
An environmental variable is considered when prioritizing patches and security responses. For example, a device in the production network environment will probably have priority over the devices in a test lab environment.

More information:
SY0-701, Objective 4.3 - Analyzing Vulnerabilities
https://professormesser.link/701040304

B46. An administrator is designing a network to be compliant with a security standard for storing credit card numbers. Which of the following would be the BEST choice to provide this compliance?

- ❍ **A.** Implement RAID for all storage systems
- ❍ **B.** Connect a UPS to all servers
- ❍ **C.** DNS should be available on redundant servers
- ❍ **D.** Perform regular audits and vulnerability scans

The Answer: D. Perform regular audits and vulnerability scans
A focus of credit card storage compliance is to keep credit card information private. The only option matching this requirement is scheduled audits and ongoing vulnerability scans.

The incorrect answers:
A. Implement RAID for all storage systems
RAID (Redundant Array of Independent Disks) is an important consideration for any project that stores data, but using a RAID array is not part of this compliance requirement. Although compliance may include backups, RAID is not a backup technology.

B. Connect a UPS to all servers
Integrating a UPS (Uninterruptible Power Supply) is an important way to maintain power during an outage, but it's not required for security compliance for data storage.

C. DNS should be available on redundant servers
Name resolution can be an important service on the network, but maintaining redundant DNS servers isn't required for compliance with sensitive data storage.

More information:
SY0-701, Objective 5.4 - Compliance
https://professormesser.link/701050401

B47. A company is accepting proposals for an upcoming project, and one of the responses is from a business owned by a board member. Which of the following would describe this situation?

- ❍ **A.** Due diligence
- ❍ **B.** Vendor monitoring
- ❍ **C.** Conflict of interest
- ❍ **D.** Right-to-audit

.....

The Answer: C. Conflict of interest
A conflict of interest occurs when a personal interest in a business transaction could compromise the judgment of the people involved. Personal and family relationships between organizations may potentially be a conflict of interest.

The incorrect answers:
A. Due diligence
Due diligence is the process of investigating and verifying information before doing business with an organization.

B. Vendor monitoring
Vendor monitoring involves ongoing management of the vendor relationship, including ongoing reviews, periodic audits, and other checks and balances.

D. Right-to-audit
A right-to-audit clause is commonly added to business contracts to ensure access to periodic audits when working with a third-party.

More information:
SY0-701, Objective 5.3 - Third-party Risk Assessment
https://professormesser.link/701050301

B48. A company has rolled out a new application that requires the use of a hardware-based token generator. Which of the following would be the BEST description of this access feature?

- ❍ **A.** Something you know
- ❍ **B.** Somewhere you are
- ❍ **C.** Something you are
- ❍ **D.** Something you have

.....

The Answer: D. Something you have
The use of the hardware token generator requires the user be in possession of the device during the login process.

The incorrect answers:
A. Something you know
The number, or token, created by the token generator isn't previously known by the user, and there's no requirement to remember the tokens once the authentication process is complete.

B. Somewhere you are
The location of an individual can be a useful authentication factor when evaluating the validity of a login request. Someone authenticating from an unexpected location or country may be subject to additional authentication checks.

C. Something you are
Something you are describes a biometric factor, such as a fingerprint or facial scan. The token generator works without any type of biometric scan.

More information:
SY0-701, Objective 4.6 - Multi-factor Authentication
https://professormesser.link/701040603

B49. A company has signed an SLA with an Internet service provider. Which of the following would BEST describe the requirements of this SLA?

- ❍ **A.** The customer will connect to remote sites over an IPsec tunnel
- ❍ **B.** The service provider will provide 99.99% uptime
- ❍ **C.** The customer applications use HTTPS over tcp/443
- ❍ **D.** Customer application use will be busiest on the 15th of each month

.....

The Answer: B. The service provider will provide 99.99% uptime
An SLA (Service Level Agreement) is a contract specifying the minimum terms for provided services. It's common to include uptime, response times, and other service metrics in an SLA.

The incorrect answers:
A. The customer will connect to remote sites over an IPsec tunnel
A service level agreement describes the minimum service levels provided to the customer. You would not commonly see descriptions of how the service will be used in the SLA contract.

C. The customer applications use HTTPS over tcp/443
The protocols used by the customer's applications aren't part of the service requirements from the ISP.

D. Customer application use will be busiest on the 15th of each month
The customer's application usage isn't part of the service requirements from the ISP.

More information:
SY0-701, Objective 5.3 - Agreement Types
https://professormesser.link/701050302

B50. An attacker has created multiple social media accounts and is posting information in an attempt to get the attention of the media. Which of the following would BEST describe this attack?

- ❍ **A.** On-path
- ❍ **B.** Watering hole
- ❍ **C.** Misinformation campaign
- ❍ **D.** Phishing

.....

The Answer: C. Misinformation campaign
Misinformation campaigns are carefully crafted attacks that exploit social media and traditional media.

The incorrect answers:
A. On-path
An on-path attack uses an attacker in the middle of a conversation to capture or modify information as it traverses the network.

B. Watering hole
A watering hole attack uses a carefully selected attack location to infect visitors to a specific website.

D. Phishing
A phishing attack uses social engineering to convince the victim to disclose private or sensitive information.

More information:
SY0-701, Objective 2.4 - Other Social Engineering Attacks
https://professormesser.link/701020205

B51. Which of the following would be the BEST way to protect credit card account information when performing real-time purchase authorizations?

- ❍ **A.** Masking
- ❍ **B.** DLP
- ❍ **C.** Tokenization
- ❍ **D.** NGFW

The Answer: C. Tokenization
Tokenization is a technique that replaces user data with a non-sensitive placeholder, or token. Tokenization is commonly used on mobile devices during a purchase to use a credit card without transmitting the physical credit card number across the network.

The incorrect answers:
A. Masking
Data masking hides sensitive data by replacing the information with a non-sensitive alternative. An example of masking would be replacing an account number on a receipt with hash marks or asterisks.

B. DLP
DLP (Data Loss Prevention) solutions can identify and block sensitive data from being sent over the network. DLP does not provide any additional security or protection for real-time financial transactions.

D. NGFW
An NGFW (Next-Generation Firewall) is an application-aware security technology. NGFW solutions can provide additional controls for specific applications, but they won't provide any additional account protections when sending financial details.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

B52. A company must comply with legal requirements for storing customer data in the same country as the customer's mailing address. Which of the following would describe this requirement?

- ❍ **A.** Geographic dispersion
- ❍ **B.** Least privilege
- ❍ **C.** Data sovereignty
- ❍ **D.** Exfiltration

The Answer: C. Data sovereignty
Data sovereignty laws can mandate how data is handled and stored. Data residing in a country is usually subject to the laws of that country, and compliance regulations may not allow the data to be moved outside of the country.

The incorrect answers:
A. Geographic dispersion
Geographic dispersion describes a data resiliency technique for distributing data to different locations to maintain uptime and availability.

B. Least privilege
Least privilege refers to a set of rights and permissions that would limit access based on a user's job requirements. Least privilege does not describe the storage of information based on a geographic location.

D. Exfiltration
Exfiltration describes the removal or theft of data by a third-party. Exfiltration is not associated with the geographic storage of information.

More information:
SY0-701, Objective 3.3 - States of Data
https://professormesser.link/701030302

B53. A company is installing access points in all of their remote sites. Which of the following would provide confidentiality for all wireless data?

- ❍ **A.** 802.1X
- ❍ **B.** WPA3
- ❍ **C.** RADIUS
- ❍ **D.** MDM

The Answer: B. WPA3
WPA3 (Wi-Fi Protected Access 3) is an encryption protocol used on wireless networks. All data sent over a WPA3-protected wireless network will be encrypted.

The incorrect answers:
A. 802.1X
802.1X is a standard for authentication using AAA (Authentication, Authorization and Accounting) services. 802.1X is commonly used in conjunction with LDAP, RADIUS, or similar authentication services.

C. RADIUS
RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol used for centralized authentication. RADIUS is commonly used in conjunction with 802.1X, but RADIUS does not provide data confidentiality or encryption.

D. MDM
An MDM (Mobile Device Manager) is used to manage and control an organization's mobile phones and tablets. MDM policies are not used to manage the confidentiality settings of a wireless access point.

More information:
SY0-701, Objective 4.1 - Wireless Security Settings
https://professormesser.link/701040104

B54. A security administrator has found a keylogger installed in an update of the company's accounting software. Which of the following would prevent the transmission of the collected logs?

- ❍ **A.** Prevent the installation of all software
- ❍ **B.** Block all unknown outbound network traffic at the Internet firewall
- ❍ **C.** Install host-based anti-virus software
- ❍ **D.** Scan all incoming email attachments at the email gateway

.....

The Answer: B. Block all unknown outbound network traffic at the Internet firewall

Keylogging software has two major functions; record user input, and transmit that information to a remote location. Local file scanning and software best-practices can help prevent the initial installation, and controlling outbound network traffic can block unauthorized file transfers.

The incorrect answers:

A. Prevent the installation of all software
Blocking software installations may prevent the initial malware infection, but it won't provide any control of outbound data.

C. Install host-based anti-virus software
A good anti-virus application can identify malware before the installation occurs, but anti-virus does not commonly provide any control of network communication.

D. Scan all incoming email attachments at the email gateway
Malware can be installed from many sources, and sometimes the source is unexpected. Scanning or blocking executables at the email gateway can help prevent infection but it won't provide any control of outbound file transfers.

More information:
SY0-701, Objective 2.4 - Other Malware Types
https://professormesser.link/701020404

B55. A user in the marketing department is unable to connect to the wireless network. After authenticating with a username and password, the user receives this message:

```
-- -- --
The connection attempt could not be completed.
The Credentials provided by the server could not be validated.
Radius Server: radius.example.com
Root CA: Example.com Internal CA Root Certificate
-- -- --
```

The access point is configured with WPA3 encryption and 802.1X authentication.

Which of the following is the MOST likely reason for this login issue?

- ❍ **A.** The user's computer is in the incorrect VLAN
- ❍ **B.** The RADIUS server is not responding
- ❍ **C.** The user's computer does not support WPA3 encryption
- ❍ **D.** The user is in a location with an insufficient wireless signal
- ❍ **E.** The client computer does not have the proper certificate installed

.....

The Answer: E. The client computer does not have the proper certificate installed

The error message states that the server credentials could not be validated. This indicates that the certificate authority that signed the server's certificate is either different than the CA certificate installed on the client's workstation, or the client workstation does not have an installed copy of the CA's certificate. This validation process ensures that the client is communicating to a trusted server and there are no on-path attacks occurring.

The incorrect answers:

A. The user's computer is in the incorrect VLAN

The RADIUS server certificate validation process should work properly from all VLANs. The error indicates that the communication process is working properly, so an incorrect VLAN would not be the cause of this issue.

B. The RADIUS server is not responding
If the RADIUS server had no response to the user, then the process would simply timeout. In this example, the error message indicates that the communication process is working between the RADIUS server and the client's computer.

C. The user's computer does not support WPA3 encryption
The first step when connecting to a wireless network is to associate with the 802.11 access point. If WPA3 encryption was not supported, the authentication process would not have occurred and the user's workstation would not have seen the server credentials.

D. The user is in a location with an insufficient wireless signal
The error message regarding server validation indicates that the wireless signal is strong enough to send and receive data on the wireless network.

More information:
SY0-701, Objective 1.4 - Certificates
https://professormesser.link/701010408

B56. A security administrator has created a new policy prohibiting the use of MD5 hashes due to collision problems. Which of the following describes the reason for this new policy?

- ❍ **A.** Two different messages have different hashes
- ❍ **B.** The original message can be derived from the hash
- ❍ **C.** Two identical messages have the same hash
- ❍ **D.** Two different messages share the same hash

.....

The Answer: D. Two different messages share the same hash
A well-designed hashing algorithm will create a unique hash value for every possible input. If two different inputs create the same hash, the hash algorithm has created a collision.

The incorrect answers:
A. Two different messages have different hashes
In normal operation, two different inputs will create two different hash outputs.

B. The original message can be derived from the hash
Hashing is a one-way cipher, and you cannot derive the original message from a hash value.

C. Two identical messages have the same hash
Two identical messages should always create exactly the same hash output.

More information:
SY0-701, Objective 2.4 - Cryptographic Attacks
https://professormesser.link/701020413

B57. A security administrator has been tasked with hardening all internal web servers to control access from certain IP address ranges and ensure all transferred data remains confidential. Which of the following should the administrator include in his project plan? (Select TWO)

- ❍ **A.** Change the administrator password
- ❍ **B.** Use HTTPS for all server communication
- ❍ **C.** Uninstall all unused software
- ❍ **D.** Enable a host-based firewall
- ❍ **E.** Install the latest operating system update

The Answer: B. Use HTTPS for all server communication, and
D. Enable a host-based firewall

Using the secure HTTPS (Hypertext Transfer Protocol Secure) protocol will ensure that all network communication is encrypted between the web server and the client devices. A host-based firewall can be used to allow or disallow traffic from certain IP address ranges.

The incorrect answers:

A. Change the administrator password
Occasionally changing administrator passwords is a good best practice, but it doesn't directly address the goals of IP address filtering and data confidentiality.

C. Uninstall all unused software
Uninstalling unused software is an important hardening technique, but uninstalling software does not control access from IP address ranges, and it does not provide any data confidentiality.

E. Install the latest operating system update
Installing an operating system update can be a useful security task, but an OS update does not directly encrypt network traffic and does not control access from certain IP addresses.

More information:
SY0-701, Objective 2.5 - Hardening Techniques
https://professormesser.link/701020503

B58. A security administrator has identified the installation of ransomware on a database server and has quarantined the system. Which of the following should be followed to ensure that the integrity of the evidence is maintained?

- ❍ **A.** E-discovery
- ❍ **B.** Non-repudiation
- ❍ **C.** Chain of custody
- ❍ **D.** Legal hold

.....

The Answer: C. Chain of custody
A chain of custody is a documented record of the evidence. The chain of custody also documents the interactions of every person who comes into contact with the evidence to maintain the integrity.

The incorrect answers:
A. E-discovery
E-discovery is the process of collecting, preparing, reviewing, interpreting, and producing electronic documents. However, e-discovery does not provide any additional integrity of the data.

B. Non-repudiation
Non-repudiation ensures the author of a document cannot be disputed. Non-repudiation does not provide any method of tracking and managing digital evidence.

D. Legal hold
A legal hold is a technique for preserving important evidence, but it doesn't provide any mechanism for the ongoing integrity of that evidence.

More information:
SY0-701, Objective 4.8 - Digital Forensics
https://professormesser.link/701040803

B59. Which of the following would be the BEST option for application testing in an environment completely separated from the production network?

- ❍ **A.** Virtualization
- ❍ **B.** VLANs
- ❍ **C.** Cloud computing
- ❍ **D.** Air gap

The Answer: D. Air gap
An air gapped network removes all connectivity between components and ensures there would be no possible communication path between the test network and the production network.

The incorrect answers:
A. Virtualization
Although virtualization provides the option to connect devices in a private network, there's still the potential for a misconfigured network configuration or an application to communicate externally.

B. VLANs
VLANs (Virtual Local Area Networks) are a common segmentation technology, but a router could easily connect the VLANs to the production network.

C. Cloud computing
Cloud-based technologies provide for many network options, and it's common to maintain a connection between the cloud and the rest of the network.

More information:
SY0-701, Objective 3.1 - Network Infrastructure Concepts
https://professormesser.link/701030102

B60. A security engineer is planning the installation of a new IPS. The network must remain operational if the IPS is turned off or disabled. Which of the following would describe this configuration?

- ❍ **A.** Containerization
- ❍ **B.** Load balancing
- ❍ **C.** Fail open
- ❍ **D.** Tunneling

.....

The Answer: C. Fail open
An IPS (Intrusion Prevention System) designed to fail open will maintain network connectivity during an outage or failure of the IPS. Even if the IPS was not actively preventing an intrusion, the network would still be up and running.

The incorrect answers:
A. Containerization
Application containerization describes the process of creating a deployment strategy where each application runs in a self-contained image. Containerization allows organizations to quickly deploy and run different application instances on the same hardware.

B. Load balancing
A load balancer will divide a single load among many different servers to provide faster response and a more efficient use of network resources. Load balancers do not maintain connectivity for an intrusion prevention system.

D. Tunneling
Tunneling describes the process of transferring data inside of another protocol type, such as sending encrypted data over a VPN (Virtual Private Network). Tunneling would not maintain network connectivity if an IPS was to fail.

More information:
SY0-701, Objective 3.2 - Intrusion Prevention
https://professormesser.link/701030202

B61. Which of the following describes the process of hiding data from others by embedding the data inside of a different media type?

- ❍ **A.** Hashing
- ❍ **B.** Obfuscation
- ❍ **C.** Encryption
- ❍ **D.** Masking

The Answer: B. Obfuscation
Obfuscation is the process of taking something normally understandable and making it very difficult to understand or to be seen. One common obfuscation method used by steganography is to embed a document within an image file.

The incorrect answers:
A. Hashing
Hashing creates a digital "fingerprint" based on the contents of data. This hash provides a method of checking data integrity, but it doesn't hide data within other media types.

C. Encryption
Encrypting source code will provide data confidentiality, but encrypting the data does not require any type of subterfuge. Conversely, hiding data within another media type does not necessarily require any type of encryption.

D. Masking
Data masking hides portions of the data by replacing it with a different value. For example, replacing a credit card number with a series of asterisks would be a common form of data masking.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

B62. Which of the following vulnerabilities would be the MOST significant security concern when protecting against a hacktivist?

- ❍ **A.** Data center access with only one authentication factor
- ❍ **B.** Spoofing of internal IP addresses when accessing an intranet server
- ❍ **C.** Employee VPN access uses a weak encryption cipher
- ❍ **D.** Lack of patch updates on an Internet-facing database server

.....

The Answer: D. Lack of patch updates on an Internet-facing database server

One of the easiest ways for a third-party to obtain information is through an existing Internet connection. A hacktivist could potentially exploit an unpatched server to obtain unauthorized access to the operating system and data.

The incorrect answers:

A. Data center access with only one authentication factor
Most hacktivists don't have access to walk around inside of your building, and they certainly wouldn't have access to secure areas. A single authentication method would commonly prevent unauthorized access to a data center for both employees and non-employees, although more authentication factors would provide additional security.

B. Spoofing of internal IP addresses when accessing an intranet server
Intranet servers are not accessible from the outside. This makes them an unlikely target for hacktivists and other non-employees.

C. Employee VPN access uses a weak encryption cipher
A weak encryption cipher can be a security issue, but a potential exploitation would require the network traffic to begin any decryption attempts. Although this scenario would technically be possible if someone was to catch an employee on a public wireless network, it's not the most significant security issue in the available list.

More information:
SY0-701, Objective 2.1 - Threat Actors
https://professormesser.link/701020101

B63. A company is installing a security appliance to protect the organization's web-based applications from attacks such as SQL injections and unexpected input. Which of the following would BEST describe this appliance?

❍ **A.** WAF

❍ **B.** VPN concentrator

❍ **C.** UTM

❍ **D.** SASE

The Answer: A. WAF
A WAF (Web Application Firewall) is designed as a firewall for web-based applications. WAFs are commonly used to protect against application attacks such as injections, cross-site scripting, and invalid input types.

The incorrect answers:
B. VPN concentrator
A VPN (Virtual Private Network) concentrator is the central connectivity point for all remote VPN users. A VPN concentrator would not be used as protection against application attacks.

C. UTM
A UTM (Unified Threat Management) appliance acts as a traditional firewall, and many UTMs may also include additional features such as intrusion prevention and content filtering. However, UTMs are not commonly used for protection of web-based applications.

D. SASE
SASE (Secure Access Service Edge) is a cloud-aware version of a VPN client, and it is commonly deployed as a client on the user device. A SASE solution would not commonly be used to protect a web-based application.

More information:
SY0-701, Objective 3.2 - Firewall Types
https://professormesser.link/701030205

B64. Which of the following would be the BEST way to determine if files have been modified after the forensics data acquisition process has occurred?

- ❍ **A.** Use a tamper seal on all storage devices
- ❍ **B.** Create a hash of the data
- ❍ **C.** Image each storage device for future comparison
- ❍ **D.** Take screenshots of file directories with file sizes

.....

The Answer: B. Create a hash of the data
A hash creates a unique value and can be quickly validated at any time in the future. If the hash value changes, then the data must have also changed.

The incorrect answers:
A. Use a tamper seal on all storage devices
A physical tamper seal will identify if a device has been opened or physically modified, but it cannot identify any changes to the data on the storage device.

C. Image each storage device for future comparison
A copy of the data would allow for comparisons later, but the process of comparing the data would take much more time than simply validating a hash value. It's also possible that someone could tamper with both the original data and the copy of the data.

D. Take screenshots of file directories with file sizes
It's very easy to change the contents of a file without changing the size of the file. Storing the file sizes would not provide any data integrity checks.

More information:
SY0-701, Objective 4.8 - Digital Forensics
https://professormesser.link/701040803

B65. A system administrator is implementing a password policy that would require letters, numbers, and special characters to be included in every password. Which of the following controls MUST be in place to enforce this password policy?

- ❍ **A.** Length
- ❍ **B.** Expiration
- ❍ **C.** Reuse
- ❍ **D.** Complexity

The Answer: D. Complexity
Adding different types of characters to a password requires technical controls that increase password complexity.

The incorrect answers:
A. Length
Adding all of these character types to a password do not necessarily change the length of the password.

B. Expiration
A common password security policy is an expiration date. This password expiration requires the user to periodically change their password.

C. Reuse
The controls that prohibit the reuse of passwords do not control the characters used in the password.

More information:
SY0-701, Objective 4.6 - Password Security
https://professormesser.link/701040604

B66. Which of the following would a company follow to deploy a weekly operating system patch?

- ❍ **A.** Tabletop exercise
- ❍ **B.** Penetration testing
- ❍ **C.** Change management
- ❍ **D.** Internal audit

The Answer: C. Change management
Change management is a formal process used to control and manage any changes to hardware, software, or any other part of the IT infrastructure.

The incorrect answers:
A. Tabletop exercise
A tabletop exercise is associated with disaster recovery planning. Instead of performing a full-scale disaster recovery test, the organization's key decision makers sit at a table and describe the steps they would follow if a disaster was to occur.

B. Penetration testing
Penetration testing is used to find vulnerabilities and other security issues. Although a penetration test might discover an unpatched system, the process of deploying the patch would be managed by the change control process.

D. Internal audit
Internal audits are important security validations, but an audit would not be used to deploy patches to company devices.

More information:
SY0-701, Objective 1.3 - Change Management Process
https://professormesser.link/701010301

B67. Which of the following would be the MOST likely result of plaintext application communication?

- ❍ **A.** Buffer overflow
- ❍ **B.** Replay attack
- ❍ **C.** Resource consumption
- ❍ **D.** Directory traversal

The Answer: B. Replay attack
To perform a replay attack, the attacker needs to capture the original non-encrypted content. If an application is not using encrypted communication, the data capture process is a relatively simple process for the attacker.

The incorrect answers:
A. Buffer overflow
A buffer overflow takes advantage of an application vulnerability and can perform this overflow over both an encrypted or non-encrypted channel.

C. Resource consumption
Resource consumption describes the use of network bandwidth or storage space, but those resource issues don't necessarily require the network communication to be sent in the clear.

D. Directory traversal
Directory traversal is commonly associated with unexpected access to the file system of a server. Non-encrypted communication is not a prerequisite in a directory traversal attack.

More information:
SY0-701, Objective 2.4 - Replay Attacks
https://professormesser.link/701020410

B68. A system administrator believes that certain configuration files on a Linux server have been modified from their original state. The administrator has reverted the configurations to their original state, but he would like to be notified if they are changed again. Which of the following would be the BEST way to provide this functionality?

- ❍ **A.** HIPS
- ❍ **B.** File integrity monitoring
- ❍ **C.** Application allow list
- ❍ **D.** WAF

The Answer: B. File integrity monitoring
File integrity monitoring software (i.e., Tripwire, System File Checker, etc.) can be used to alert if the contents of a file are modified.

The incorrect answers:
A. HIPS
The use of HIPS (Host-based Intrusion Prevention System) would help identify any security vulnerabilities, but there's nothing relating to this issue that would indicate it was caused by an operating system or application vulnerability. A HIPS would not commonly alert on the modification of a specific file.

C. Application allow list
In this example, we're not sure how the file was changed or if a separate application or editor was used. If the change was made with a valid application, an allow list would not provide any feedback or alerts.

D. WAF
A WAF (Web Application Firewall) is used to protect web-based applications from malicious attack. The example in this question was not related to a web-based application.

More information:
SY0-701, Objective 4.5 - Monitoring Data
https://professormesser.link/701040506

B69. A security administrator is updating the network infrastructure to support 802.1X. Which of the following would be the BEST choice for this configuration?

- ❍ **A.** LDAP
- ❍ **B.** SIEM
- ❍ **C.** SNMP traps
- ❍ **D.** SPF

The Answer: A. LDAP
802.1X is a standard for authentication, and LDAP (Lightweight Directory Access Protocol) is a common protocol used for centralized authentication. Other protocols such as RADIUS, TACACS+, or Kerberos would also be options for 802.1X authentication.

The incorrect answers:
B. SIEM
A SIEM (Security Information and Event Management) system is designed to consolidate log files from multiple devices, quickly search through data, and create long-term reports. A SIEM does not provide any additional functionality for the authentication process.

C. SNMP traps
SNMP (Simple Network Management Protocol) traps are used to provide alerts and alarms from servers and infrastructure devices. SNMP is not an authentication protocol.

D. SPF
SPF (Sender Policy Framework) is an email security standard used to validate authorized mail senders. The SPF information is added to a DNS (Domain Name System) server and accessed by email recipients.

More information:
SY0-701, Objective 4.6 - Identity and Access Management
https://professormesser.link/701040601

B70. A company owns a time clock appliance, but the time clock doesn't provide any access to the operating system and it doesn't provide a method to upgrade the firmware. Which of the following describes this appliance?

- ❍ **A.** End-of-life
- ❍ **B.** ICS
- ❍ **C.** SDN
- ❍ **D.** Embedded system

The Answer: D. Embedded system
An embedded system often does not provide access to the OS and may not provide a method of upgrading the system firmware.

The incorrect answers:
A. End-of-life
A device at its end-of-life is no longer supported by the vendor. In this example, the vendor support status isn't mentioned.

B. ICS
ICS (Industrial Control Systems) devices are large industrial systems and usually involve manufacturing equipment or power generation equipment. A time clock would not be categorized as an ICS.

C. SDN
An SDN (Software Defined Network) is commonly used as a method of deploying network components by separating a device into a data plane, control plane, and management plane. A time clock appliance would not be categorized as an SDN.

More information:
SY0-701, Objective 3.1 - Other Infrastructure Concepts
https://professormesser.link/701030103

B71. A company has deployed laptops to all employees, and each laptop is enumerated during each login. Which of the following is supported with this configuration?

- ❍ **A.** If the laptop hardware is modified, the security team is alerted
- ❍ **B.** Any malware identified on the system is automatically deleted
- ❍ **C.** Users are required to use at least two factors of authentication
- ❍ **D.** The laptop is added to a private VLAN after the login process

The Answer: A. If the laptop hardware is modified, the security team is alerted

The enumeration process identifies and reports on the hardware and software installed on the laptop. If this configuration is changed, an alert can be generated.

The incorrect answers:

B. Any malware identified on the system is automatically deleted
Although it's very likely the laptop is running some type of anti-malware software, this question was regarding the enumeration process.

C. Users are required to use at least two factors of authentication
It's always a good idea to support multifactor authentication, but the enumeration process does not support any additional authentication factors.

D. The laptop is added to a private VLAN after the login process
Many organizations can identify the login and automatically move that device to the correct VLANs. The enumeration mentioned does not provide this functionality.

More information:
SY0-701, Objective 4.2 - Asset Management
https://professormesser.link/701040201

B72. A security manager believes that an employee is using their laptop to circumvent the corporate Internet security controls through the use of a cellular hotspot. Which of the following could be used to validate this belief? (Select TWO)

- ❍ **A.** HIPS
- ❍ **B.** UTM logs
- ❍ **C.** Web application firewall events
- ❍ **D.** Host-based firewall logs
- ❍ **E.** Next-generation firewall logs

.....

The Answer: A. HIPS and **D.** Host-based firewall logs
If the laptop is not communicating across the corporate network, then the only evidence of the traffic would be contained on the laptop itself. A HIPS (Host-based Intrusion Prevention System) logs and host-based firewall logs may contain information about recent traffic flows to systems outside of the corporate network.

The incorrect answers:
B. UTM logs
A unified threat management appliance is commonly located in the core of the network. The use of a cellular hotspot would circumvent the UTM and this traffic would not be logged.

C. Web application firewall events
Web application firewalls are commonly used to protect internal web servers. Outbound Internet communication would not be logged, and anyone circumventing the existing security controls would also not be logged.

E. Next-generation firewall logs
Although a next-generation firewall keeps detailed logs, any systems communicating outside of the normal corporate Internet connection would not appear in those logs.

More information:
SY0-701, Objective 2.5 - Hardening Techniques
https://professormesser.link/701020503

B73. An application developer is creating a mobile device app that will require a true random number generator real-time memory encryption. Which of the following technologies would be the BEST choice for this app?

- ❍ **A.** HSM
- ❍ **B.** Secure enclave
- ❍ **C.** NGFW
- ❍ **D.** Self-signed certificates

.....

The Answer: B. Secure enclave
A secure enclave describes a hardware processor designed for security. The secure enclave monitors the boot process, create true random numbers, store root cryptography keys, and much more.

The incorrect answers:
A. HSM
An HSM (Hardware Security Module) is often implemented as a high-end cryptographic hardware appliance. HSMs are often used as secure storage for cryptographic keys.

C. NGFW
An NGFW (Next Generation Firewall) is an application aware firewall and is commonly used to manage traffic flows. An NGFW would not be able to provide true random numbers or real-time memory encryption on a device.

D. Self-signed certificates
A self-signed certificate is a digital certificate created on a private Certificate Authority and digitally signed by the private CA. A certificate does not provide randomization functions or memory encryption capabilities.

More information:
SY0-701, Objective 1.4 - Encryption Technologies
https://professormesser.link/701010404

B74. Which of the following would be a common result of a successful vulnerability scan?

- ❍ **A.** Usernames and password hashes from a server
- ❍ **B.** A list of missing software patches
- ❍ **C.** A copy of image files from a private file share
- ❍ **D.** The BIOS configuration of a server

The Answer: B. A list of missing software patches
A vulnerability scan can identify vulnerabilities and list the patches associated with those vulnerabilities.

The incorrect answers:
A. Usernames and password hashes from a server
This type of secure information cannot be obtained through a vulnerability scan.

C. A copy of image files from a private file share
A private file share would prevent any access by unauthorized users, and a vulnerability scan would not have access to private data.

D. The BIOS configuration of a server
Private information, such as a device's BIOS configuration, is not available from a vulnerability scan.

More information:
SY0-701, Objective 4.3 - Vulnerability Scanning
https://professormesser.link/701040301

B75. When connected to the wireless network, users at a remote site receive an IP address which is not part of the corporate address scheme. Communication over this network is also slower than the wireless connections elsewhere in the building. Which of the following would be the MOST likely reason for these issues?

- ❍ **A.** Rogue access point
- ❍ **B.** Domain hijack
- ❍ **C.** DDoS
- ❍ **D.** Encryption is enabled

.....

The Answer: A. Rogue access point
A rogue access point is an unauthorized access point added by a user or attacker. This access point may not necessarily be malicious, but it does create significant security concerns and unauthorized access to the corporate network.

The incorrect answers:
B. Domain hijack
A domain hijacking would be associated with unauthorized access to a domain name. In this example, the wireless IP addressing and performance issues do not appear to be related to a domain hijack.

C. DDoS
A DDOS (Distributed Denial of Service) would cause outages or slow performance to a service. A DDoS would not commonly modify or update any local IP addresses.

D. Encryption is enabled
Wireless encryption protocols are relatively efficient and do not contribute to a significant delay of network traffic. An encrypted wireless network would also not assign IP addresses outside of the expected range.

More information:
SY0-701, Objective 2.2 - Common Threat Vectors
https://professormesser.link/701020201

B76. A company has identified a compromised server, and the security team would like to know if an attacker has used this device to move between systems. Which of the following would be the BEST way to provide this information?

- ❍ **A.** DNS server logs
- ❍ **B.** Penetration test
- ❍ **C.** NetFlow logs
- ❍ **D.** Email metadata

.....

The Answer: C. NetFlow logs
NetFlow information can provide a summary of network traffic, application usage, and details of network conversations. The NetFlow logs will show all conversations from this device to any others in the network.

The incorrect answers:
A. DNS server logs
DNS server logs will document all name resolutions, but an attacker may not be using a DNS server and may prefer accessing devices by IP address.

B. Penetration test
A penetration test may identify any vulnerabilities that exist on the server, but it won't provide any information about traffic flows or connections initiated by an attacker.

D. Email metadata
An email header contains the IP addresses of email servers used to transfer the message, and security signatures to verify the sender. The metadata in an email header would not contain information on traffic flows associated with this attacker.

More information:
SY0-701, Objective 4.4 - Security Tools
https://professormesser.link/701040402

B77. A system administrator has protected a set of system backups with an encryption key. The system administrator used the same key when restoring files from this backup. Which of the following would BEST describe this encryption type?

- ❍ **A.** Asymmetric
- ❍ **B.** Key escrow
- ❍ **C.** Symmetric
- ❍ **D.** Out-of-band key exchange

The Answer: C. Symmetric
Symmetric encryption uses the same key for both encryption and decryption.

The incorrect answers:
A. Asymmetric
Asymmetric encryption uses different keys for encryption and decryption.

B. Key escrow
Key escrow describes a third-party which holds the decryption keys for your data.

D. Out-of-band key exchange
Keys can be transferred between people or systems over the network (in-band) or outside the normal network communication (out-of-band). In this example, the key wasn't exchanged between people or systems, since the system administrator is the same person who encrypted and decrypted.

More information:
SY0-701, Objective 1.4 - Public Key Infrastructure
https://professormesser.link/701010401

B78. A new malware variant takes advantage of a vulnerability in a popular email client. Once installed, the malware forwards all email attachments with credit card information to an external email address. Which of the following would limit the scope of this attack?

- ❍ **A.** Enable MFA on the email client
- ❍ **B.** Scan outgoing traffic with DLP
- ❍ **C.** Require users to enable the VPN when using email
- ❍ **D.** Update the list of malicious URLs in the firewall

.....

The Answer: B. Scan outgoing traffic with DLP
DLP (Data Loss Prevention) systems are designed to identify sensitive data transfers. If the DLP finds a data transfer with financial details, personal information, or other private information, the DLP can block the data transfer.

The incorrect answers:
A. Enable MFA on the email client
MFA (Multi-Factor Authentication) can provide more security during the authentication process, but the description of the malware did not associate the exploit with the login process. The malware will most likely wait for the user to login before transferring the data.

C. Require users to enable the VPN when using email
A VPN (Virtual Private Network) can protect data between systems, but it won't prevent malware from sending data once it connects to the email system.

D. Update the list of malicious URLs in the firewall
Blocking known URLs (Uniform Resource Locators) in a firewall is a useful way to prevent access to known malicious sites, but it won't prevent malware from sending email messages.

More information:
SY0-701, Objective 4.5 - Monitoring Data
https://professormesser.link/701040506

B79. An organization has identified a security breach and has removed the affected servers from the network. Which of the following is the NEXT step in the incident response process?

- ❍ **A.** Eradication
- ❍ **B.** Preparation
- ❍ **C.** Recovery
- ❍ **D.** Detection
- ❍ **E.** Containment

.....

The Answer: A. Eradication
The incident response process is preparation, detection, analysis, containment, eradication, recovery, and lessons learned. Once a system has been contained, any malware or breached user accounts should be removed from the system.

The incorrect answers:
B. Preparation
Before an incident occurs, you should compile contact information, incident handling hardware and software, analysis resources, and other important tools and policies.

C. Recovery
The focus of the recovery process is to get all of the systems back to normal. This phase removes malware, deletes breached user accounts, and fixes any vulnerabilities.

D. Detection
Detection of an event can be challenging, but it usually consists of IPS reports, anti-virus alerts, configuration change notifications, and other indicators.

E. Containment
In this example, the containment and isolation occurred when the affected servers were removed from the network.

More information:
SY0-701, Objective 4.8 - Incident Response
https://professormesser.link/701040801

B80. A security administrator has been tasked with storing and protecting customer payment and shipping information for a three-year period. Which of the following would describe the source of this data?

- ❍ **A.** Controller
- ❍ **B.** Owner
- ❍ **C.** Data subject
- ❍ **D.** Processor

.....

The Answer: C. Data subject
In data privacy, the data subject describes an individual with personal data. Payment details and shipping addresses describe personal information from a data subject.

The incorrect answers:
A. Controller
A data controller manages the processing of the data. A payroll department would be an example of a data controller.

B. Owner
The data owner is commonly accountable for all of the data, and the owner often manages the people and systems associated with processing and securing the data.

D. Processor
A data processor manages the data on behalf of the data controller. If the data controller is the payroll department, a third-party payroll company would be the data processor.

More information:
SY0-701, Objective 5.4 - Privacy
https://professormesser.link/701050402

B81. Which of the following would be the main reasons why a system administrator would use a TPM when configuring full disk encryption? (Select TWO)

- ❍ **A.** Allows the encryption of multiple volumes
- ❍ **B.** Uses burned-in cryptographic keys
- ❍ **C.** Stores certificates in a hardware security module
- ❍ **D.** Maintains a copy of the CRL
- ❍ **E.** Includes built-in protections against brute-force attacks

The Answer: B. Uses burned-in cryptographic keys and
E. Includes built-in protections against brute-force attacks

A TPM (Trusted Platform Module) is part of a computer's motherboard, and it's specifically designed to assist and protect with cryptographic functions. Full disk encryption (FDE) can use the burned-in TPM keys to verify the local device hasn't changed, and there are security features in the TPM to prevent brute-force or dictionary attacks against the full disk encryption login credentials.

The incorrect answers:

A. Allows the encryption of multiple volumes
The use of a TPM is not associated with the number of volumes encrypted with FDE.

C. Stores certificates in a hardware security module
A hardware security module (HSM) is high-end cryptographic hardware specifically designed for large-scale secured storage on the network. An HSM server is a separate device and is not associated with an individual device's TPM.

D. Maintains a copy of the CRL
A CRL (Certificate Revocation List) is maintained by the Certificate Authority and is not part of the TPM.

More information:
SY0-701, Objective 3.2 - Encryption Technologies
https://professormesser.link/701010404

B82. A security administrator is using an access control where each file or folder is assigned a security clearance level, such as "confidential" or "secret." The security administrator then assigns a maximum security level to each user. What type of access control is used in this network?

- ❍ **A.** Mandatory
- ❍ **B.** Rule-based
- ❍ **C.** Discretionary
- ❍ **D.** Role-based

The Answer: A. Mandatory
Mandatory access control uses a series of security levels (i.e., public, private, secret) and assigns those levels to each object in the operating system. Users are assigned a security level, and they would only have access to objects that meet or are below that assigned security level.

The incorrect answers:
B. Rule-based
Rule-based access control determines access based on a series of system-enforced rules. An access rule might require a particular browser be used to complete a web page form, or access to a file or system is only allowed during certain times of the day.

C. Discretionary
Discretionary access control allows the owner of an object to assign access. If a user creates a spreadsheet, the user can then assign users and groups to have a particular level of access to that spreadsheet.

D. Role-based
Role-based access control assigns a user's permissions based on their role in the organization. For example, a manager would have a different set of rights and permissions than a team lead.

More information:
SY0-701, Objective 4.6 - Access Controls
https://professormesser.link/701040602

B83. A security administrator is reviewing a report showing a number of devices on internal networks are connecting with servers in the data center network. Which of the following security systems should be added to prevent internal systems from accessing data center devices?

- ❍ **A.** VPN
- ❍ **B.** IPS
- ❍ **C.** SIEM
- ❍ **D.** ACL

The Answer: D. ACL
An ACL (Access Control List) is a security control commonly implemented on routers to allow or restrict traffic flows through the network.

The incorrect answers:
A. VPN
A VPN (Virtual Private Network) can be used to secure data traversing the network, but it's not commonly used to control traffic flows on an internal network.

B. IPS
An IPS (Intrusion Prevention System) is designed to identify and block known vulnerabilities traversing the network. An IPS is not used to control other traffic flows.

C. SIEM
A SIEM (Security Information and Event Management) server is commonly used to consolidate and report on log files. A SIEM would not be able to control or limit network communication.

More information:
SY0-701, Objective 2.5 - Segmentation and Access Control
https://professormesser.link/701020501

B84. A financial services company is headquartered in an area with a high occurrence of tropical storms and hurricanes. Which of the following would be MOST important when restoring services disabled by a storm?

- ❍ **A.** Disaster recovery plan
- ❍ **B.** Stakeholder management
- ❍ **C.** Change management
- ❍ **D.** Retention policies

.....

The Answer: A. Disaster recovery plan
A disaster recovery plan is a comprehensive set of processes for large-scale outages that affect the organization. Natural disasters, technology failures, and human-created disasters would be reasons to implement a disaster recovery plan.

The incorrect answers:
B. Stakeholder management
Stakeholder management describes the relationship IT has with the their customers. Although stakeholder management is common for the change control process, the priority after a major event is to start the disaster recovery process.

C. Change management
Change management is an important process when making any type of planned and expected change to the infrastructure. When a tropical storm affects uptime and availability, the disaster recovery plan would be the better choice.

D. Retention policies
Retention policies specify the type and amount of data that must be backed up and stored. These policies are often self-imposed or part of a larger set of rules and regulations.

More information:
SY0-701, Objective 4.2 - Incident Response Planning
https://professormesser.link/601040202

B85. A user in the mail room has reported an overall slowdown of his shipping management software. An anti-virus scan did not identify any issues, but a more thorough malware scan identified a kernel driver which is not part of the original operating system installation. Which of the following malware was installed on this system?

- ❍ **A.** Rootkit
- ❍ **B.** Logic bomb
- ❍ **C.** Bloatware
- ❍ **D.** Ransomware
- ❍ **E.** Keylogger

.....

The Answer: A. Rootkit
A rootkit often modifies core system files and becomes effectively invisible to the rest of the operating system. The modification of system files and specialized kernel-level drivers are common rootkit techniques.

The incorrect answers:
B. Logic bomb
A logic bomb waits for a predefined event, and then executes at that event time. This event may be a time of day, a user event, or any other identifiable event.

C. Bloatware
Bloatware consists of apps which have been preinstalled onto new phones, tablets, or computers. Some of these apps can create resource contention for CPU time, memory capacity, or free storage space.

D. Ransomware
Ransomware makes itself quite visible on your system, and it usually presents warning messages and information on how to remove the ransomware from the system.

E. Keylogger
A keylogger captures keyboard and mouse input and sends that information to another device. This usually means the keylogger has a visible component in the list of processes, and the keylogger traffic can often be seen on the network.

More information:
SY0-701, Objective 2.4 - Other Malware Types
https://professormesser.link/701020404

B86. A virus scanner has identified a macro virus in a word processing file attached to an email. Which of the following information could be obtained from the metadata of this file?

- ❍ **A.** IPS signature name and number
- ❍ **B.** Operating system version
- ❍ **C.** Date and time when the file was created
- ❍ **D.** Alert disposition

.....

The Answer: C. Date and time when the file was created
The data and time the file was created is commonly found in the metadata of the document.

The incorrect answers:
A. IPS signature name and number
The metadata is stored in the word processing file, and the IPS will not change the information stored in the file or appear anywhere in the document itself.

B. Operating system version
Word processing files are not specific to an operating system, so it would not be common to find OS information stored in the metadata of a word processing file.

D. Alert disposition
The alert information created when the macro virus was discovered would not be included as part of the word processing file metadata.

More information:
SY0-701, Objective 4.9 - Log Data
https://professormesser.link/701040901

B87. When a person enters a data center facility, they must check-in before they are allowed to move further into the building. People who are leaving must be formally checked-out before they are able to exit the building. Which of the following would BEST facilitate this process?

- ❍ **A.** Access control vestibule
- ❍ **B.** Air gap
- ❍ **C.** Pressure sensors
- ❍ **D.** Bollards

The Answer: A. Access control vestibule
An access control vestibule is commonly used to control the flow of people through a particular area. Unlocking the one door of the vestibule commonly restricts the other door from opening, thereby preventing someone from walking through without stopping. It's common in large data centers to have a single room as the access control vestibule where users are checked in and out of the facility.

The incorrect answers:
B. Air gap
An air gap is a security control that creates a physical separation between devices or networks. An air gap is not used to manage the flow of people.

C. Pressure sensors
A pressure sensor detects a change in force, and they are commonly used for floor and window sensors. Pressure sensors are not used for the check-in process at a data center.

D. Bollards
Bollards are often used to channel people through a specific access point and prevent vehicles from entering the area. Bollards may help to protect the outside of a data center building, but bollards are not used as access control devices for data centers or other secure facilities.

More information:
SY0-701, Objective 1.2 - Physical Security
https://professormesser.link/701010206

B88. A security administrator has discovered an employee exfiltrating confidential company information by embedding data within image files and emailing the images to a third-party. Which of the following would best describe this activity?

- ❍ **A.** Digital signatures
- ❍ **B.** Steganography
- ❍ **C.** Salting
- ❍ **D.** Data masking

The Answer: B. Steganography
Steganography is the process of hiding information within another document. For example, one common method of steganography embeds data or documents within image files.

The incorrect answers:
A. Digital signatures
A digital signature is a cryptographic method used to check the integrity, authentication, and non-repudiation of a message. Digital signatures are not used to hide information within image files.

C. Salting
Salting adds information the hashing process to ensure a unique hash value. The salting process does not involve embedding or hiding data within other types of media.

D. Data masking
Data masking replaces the display of sensitive information with another value. Replacing a credit card number on a receipt with a series of asterisks would be an example of data masking.

More information:
SY0-701, Objective 1.4 - Obfuscation
https://professormesser.link/701010405

B89. A third-party has been contracted to perform a penetration test on a company's public web servers. The testing company has been provided with the external IP addresses of the servers. Which of the following would describe this scenario?

- ❍ **A.** Defensive
- ❍ **B.** Active reconnaissance
- ❍ **C.** Partially known environment
- ❍ **D.** Regulatory

The Answer: C. Partially known environment
A partially known environment provides limited information about the testing systems and networks during a penetration test.

The incorrect answers:
A. Defensive
A defensive approach to penetration tests usually involves the blue team identifying incoming attacks in real-time.

B. Active reconnaissance
Active reconnaissance gathers information which could be visible on network traffic logs and packet captures. The IP addresses of the servers were provided by the client and are not part of a reconnaissance process.

D. Regulatory
Some organizations may be required by regulation to perform ongoing vulnerability scans and security tasks. There's no mention in this question regarding any legal or regulatory requirements.

More information:
SY0-701, Objective 5.5 - Penetration Tests
https://professormesser.link/701050502

B90. Which of the following would be the best way to describe the estimated number of laptops that might be stolen in a fiscal year?

- ❍ **A.** ALE
- ❍ **B.** SLE
- ❍ **C.** ARO
- ❍ **D.** MTTR

The Answer: C. ARO
The ARO (Annualized Rate of Occurrence) describes the number of instances estimated to occur in a year. For example, if the organization expect to lose seven laptops to theft in a year, the ARO for laptop theft is seven.

The incorrect answers:
A. ALE
The ALE (Annual Loss Expectancy) is the expected cost for all events in a single year. If it costs $1,000 to replace a single laptop (the SLE) and you expect to lose seven laptops in a year (the ARO), the ALE for laptop theft is $7,000.

B. SLE
SLE (Single Loss Expectancy) is the monetary loss if a single event occurs. If one laptop is stolen, the cost to replace that single laptop is the SLE, or $1,000.

D. MTTR
MTTR (Mean Time to Repair) is the time required to repair a product or system after a failure.

More information:
SY0-701, Objective 5.2 - Risk Analysis
https://professormesser.link/701050202

C6. A finance company is legally required to maintain seven years of tax records for all of their customers. Which of the following would be the BEST way to implement this requirement?

- ❍ **A.** Automate a script to remove all tax information more than seven years old
- ❍ **B.** Print and store all tax records in a seven-year cycle
- ❍ **C.** Allow users to download tax records from their account login
- ❍ **D.** Create a separate daily backup archive for all applicable tax records

The Answer: D. Create a separate daily backup archive for all applicable tax records

An important consideration for a data retention mandate is to always have access to the information over the proposed time frame. In this example, a daily backup would ensure tax information is constantly archived over a seven year period and could always be retrieved if needed. If data was inadvertently deleted from the primary storage, the backup would still maintain a copy.

The incorrect answers:

A. Automate a script to remove all tax information more than seven years old

The requirement is to maintain data for at least seven years, but there's no requirement to remove that data after that time frame. For example, some financial information may need to be retained well beyond the seven year mandate.

B. Print and store all tax records in a seven-year cycle

Paper has its place, but creating physical output of tax records and storing them for seven years would include a significant cost in time, materials, and inventory space. The requirement to store data for seven years doesn't require the information to be stored in a physical form.

C. Allow users to download tax records from their account login

Including a feature to allow access to their records is useful for the user community, but it doesn't provide any data protection for the seven year retention period.

More information:
SY0-701, Objective 4.2 - Asset Management
https://professormesser.link/701040201

C7. A system administrator is designing a data center for an insurance company's new public cloud and would like to automatically rotate encryption keys on a regular basis. Which of the following would provide this functionality?

- ❍ **A.** TPM
- ❍ **B.** Key management system
- ❍ **C.** Secure enclave
- ❍ **D.** XDR

.....

The Answer: B. Key management system
A key management system is used to manage large security key implementations from a central console. This includes creating keys, associating keys with individuals, rotating keys on regular intervals, and logging all key use.

The incorrect answers:
A. TPM
A TPM (Trusted Platform Module) provides cryptographic features on a hardware device. TPMs are often integrated onto the motherboard or system board of an individual device or component.

C. Secure enclave
A secure enclave is usually implemented as a cryptographic hardware processor and provides extensive security features for a device.

D. XDR
XDR (Extended Detection and Response) clients are often installed onto user devices to correlate endpoint, network, and cloud data to identify malicious software and attacks.

More information:
SY0-701, Objective 1.4 - Encryption Technologies
https://professormesser.link/701010404

C8. A newly installed IPS is flagging a legitimate corporate application as malicious network traffic. Which of the following would be the BEST way to resolve this issue?

- ❍ **A.** Disable the IPS signature
- ❍ **B.** Block the application
- ❍ **C.** Log all IPS events
- ❍ **D.** Tune the IPS alerts

The Answer: D. Tune the IPS alerts
Each signature of an IPS can commonly be tuned to properly alert on a legitimate issue. Tuning the IPS can properly identify and block attacks and allow all legitimate traffic.

The incorrect answers:
A. Disable the IPS signature
Disabling the IPS signature would certainly remove the alerts, but it also would prevent the IPS from blocking an actual attack.

B. Block the application
Blocking the corporate application would be an unusual response, especially when the application is legitimate and does not pose a security concern.

C. Log all IPS events
It's useful to log all security events, but simply logging the events doesn't correct the false positive report.

More information:
SY0-701, Objective 4.4 - Security Monitoring
https://professormesser.link/701040401

C9. A security administrator has identified an internally developed application which allows modification of SQL queries through the web-based front-end. Which of the following changes would resolve this vulnerability?

- ❍ **A.** Store all credentials as salted hashes
- ❍ **B.** Verify the application's digital signature
- ❍ **C.** Validate all application input
- ❍ **D.** Obfuscate the application's source code

.....

The Answer: C. Validate all application input
Input validation would examine the input from the client and make sure that the input is expected and not malicious. In this example, validating the input would prevent any SQL (Structured Query Language) injection through the web front-end.

The incorrect answers:
A. Store all credentials as salted hashes
Although credential storage should commonly be salted and hashed, changing the process for storing passwords would not resolve any issues related to application input.

B. Verify the application's digital signature
Code that has been digitally signed by the application developer can be evaluated to ensure that nothing has changed with the application code since it was published, but it would not prevent any type of code injection.

D. Obfuscate the application's source code
Obfuscation makes something normally understandable very difficult to understand. Obfuscating the source code of the application would make it much more difficult to read, but it wouldn't prevent a SQL injection.

More information:
SY0-701, Objective 4.1 - Application Security
https://professormesser.link/701040105

C10. A system administrator is implementing a fingerprint scanner to provide access to the data center. Which of the following authentication technologies would be associated with this access?

- ❍ **A.** Digital signature
- ❍ **B.** Hard authentication token
- ❍ **C.** Security key
- ❍ **D.** Something you are

The Answer: D. Something you are
An authentication factor of "something you are" often refers to a physical characteristic. This factor commonly uses fingerprints, facial recognition, or some other biometric characteristic to match a user to an authentication attempt.

The incorrect answers:
A. Digital signature
A digital signature is a cryptographic method used to verify the source and contents of data. Adding a fingerprint scanner would not provide a digital signature.

B. Hard authentication token
Many software-based authentication tokens are available for our mobile phones and tablets, but there are also stand-alone hard authentication tokens that are often attached to a keyring or lanyard.

C. Security key
A USB (Universal Serial Bus) security key commonly stores a digital signature for authentication or user verification. A USB key is not commonly part of a fingerprint scanner.

More information:
SY0-701, Objective 4.6 - Multi-factor Authentication
https://professormesser.link/701040603

C11. The IT department of a transportation company maintains an on-site inventory of chassis-based network switch interface cards. If a failure occurs, the on-site technician can replace the interface card and have the system running again in sixty minutes. Which of the following BEST describes this recovery metric?

- ❍ **A.** MTBF
- ❍ **B.** MTTR
- ❍ **C.** RPO
- ❍ **D.** RTO

.....

The Answer: B. MTTR
MTTR (Mean Time To Restore) is the amount of time required to get back up and running. This is sometimes called Mean Time To Repair.

The incorrect answers:
A. MTBF
MTBF (Mean Time Between Failures) is a prediction of how long the system will be operational before a failure occurs.

C. RPO
An RPO (Recovery Point Objective) is a qualifier that determines when the system is recovered. A recovered system may not be completely repaired, but it will be running well enough to maintain a certain level of operation.

D. RTO
An RTO (Recovery Time Objective) is the service level goal to work towards when recovering a system and getting back up and running.

More information:
SY0-701, Objective 5.2 - Business Impact Analysis
https://professormesser.link/701050204

C12. A company maintains a server farm in a large data center. These servers are used internally and are not accessible from outside of the data center. The security team has discovered a group of servers was breached before the latest security patches were applied. Breach attempts were not logged on any other servers. Which of these threat actors would be MOST likely involved in this breach?

❍ **A.** Organized crime

❍ **B.** Insider

❍ **C.** Nation state

❍ **D.** Unskilled attacker

The Answer: B. Insider
None of these servers are accessible from the outside, and the only servers with any logged connections were also susceptible to the latest vulnerabilities. To complete this attack, there would need a very specific knowledge of the vulnerable systems and a way to communicate with those servers.

The incorrect answers:
A. Organized crime
Organized crime can be very effective at hacking systems and companies, but they can only affect systems where they have access. Internal servers would not be accessible to anyone on the outside of the organization.

C. Nation state
A nation state would have the resources needed to attack a network, gain access to the internal systems, and then somehow monitor the update processes for each server. However, the scope and breadth of such an attack would be complex, and this would make the nation state a very speculative option and not the most likely choice from the available list.

D. Unskilled attacker
Unskilled attackers don't usually have access to an internal network, and they generally aren't knowledgeable enough to track the status of which systems may have been recently updated.

More information:
SY0-701, Objective 2.1 - Threat Actors
https://professormesser.link/701020101

C13. An organization has received a vulnerability scan report of their Internet-facing web servers. The report shows the servers have multiple Sun Java Runtime Environment (JRE) vulnerabilities, but the server administrator has verified that JRE is not installed. Which of the following would be the BEST way to handle this report?

- ❍ **A.** Install the latest version of JRE on the server
- ❍ **B.** Quarantine the server and scan for malware
- ❍ **C.** Harden the operating system of the web server
- ❍ **D.** Ignore the JRE vulnerability alert

.....

The Answer: D. Ignore the JRE vulnerability alert
It's relatively common for vulnerability scans to show vulnerabilities that don't actually exist, especially if the scans are not credentialed. An issue that is identified but does not actually exist is a false positive, and it can be dismissed once the alert has been properly researched.

The incorrect answers:
A. Install the latest version of JRE on the server
The system administrator verified that JRE was not currently installed on the server, so it would not be possible for that vulnerability to actually exist. Installing an unneeded version of JRE on the server could potentially open the server to actual vulnerabilities.

B. Quarantine the server and scan for malware
The JRE false positive isn't an indication of malware, and there's no mention of any additional vulnerabilities or reports of malware.

C. Harden the operating system of the web server
Although it's always a good best practice to harden the operating system of an externally-facing server, this vulnerability scan report doesn't indicate any particular vulnerability with the operating system itself. If the scan identified specific OS vulnerabilities, then additional hardening may be required.

More information:
SY0-701, Objective 4.3 - Analyzing Vulnerabilities
https://professormesser.link/701040304

C14. A user downloaded and installed a utility for compressing and decompressing files. Immediately after installing the utility, the user's overall workstation performance degraded and it now takes twice as much time to perform any tasks on the computer. Which of the following is the BEST description of this malware infection?

- ❍ **A.** Ransomware
- ❍ **B.** Bloatware
- ❍ **C.** Logic bomb
- ❍ **D.** Trojan

The Answer: D. Trojan
A Trojan horse is malicious software that pretends to be something benign. The user will install the software with the expectation that it will perform a particular function, but in reality it is installing malware on the computer.

The incorrect answers:
A. Ransomware
Ransomware will lock a system and present a message to the user with instructions on how to unlock the system. This usually involves sending the attacker money in exchange for the unlock key.

B. Bloatware
Bloatware is delivered as numerous and often unnecessary applications which have been pre-installed to a system.

C. Logic bomb
A logic bomb will execute when a certain event occurs, such as a specific date and time.

More information:
SY0-701, Objective 2.4 - An Overview of Malware
https://professormesser.link/701020401

C15. Which of the following is the process for replacing sensitive data with a non-sensitive and functional placeholder?

- ❍ **A.** Steganography
- ❍ **B.** Tokenization
- ❍ **C.** Retention
- ❍ **D.** Masking

The Answer: B. Tokenization
Tokenization replaces sensitive data with a token, and this token can be used as a functional placeholder for the original data. Tokenization is commonly used with credit card processing and mobile devices.

The incorrect answers:
A. Steganography
Steganography is a method of hiding data within another media type. For example, one common type of steganography is hiding information within a digital image.

C. Retention
Data retention specifies the amount of time that data should be stored or saved. Retention policies do not commonly replace sensitive data.

D. Masking
Data masking hides some of the original data to protect it from view. While hidden, this data cannot be used for any functional purpose.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

C16. A security administrator has installed a new firewall to protect a web server VLAN. The application owner requires all web server sessions communicate over an encrypted channel. Which rule should the security administrator add to the firewall rulebase?

❍ **A.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 23, Deny`

❍ **B.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 22, Allow`

❍ **C.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Allow`

❍ **D.** `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Allow`

.....

The Answer:

D. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 443, Allow`

Most web servers use tcp/443 for HTTPS (Hypertext Transfer Protocol Secure) for encrypted web server communication This rule allows HTTPS encrypted traffic to be forwarded to the web server over tcp/443.

The incorrect answers:

A. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 23, Deny`
The insecure Telnet protocol commonly uses tcp/23, but most web servers would not be listening on tcp/23. An explicit tcp/23 deny rule would not provide any additional web server security.

B. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 22, Allow`
The SSH (Secure Shell) protocol uses tcp/22 to provide encrypted terminal communication, but the web server does not use SSH when communicating with client web browsers.

E. `Source: ANY, Destination: ANY, Protocol: TCP, Port: 80, Allow`
Unencrypted web communication commonly uses tcp/80. Since the application owner requires encrypted communication, allowing HTTP over tcp/80 should not be allowed through the firewall.

More information:
SY0-701, Objective 4.5 - Firewalls
https://professormesser.link/701040501

C17. Which of these would be used to provide multi-factor authentication?

- ❍ **A.** USB-connected storage drive with FDE
- ❍ **B.** Employee policy manual
- ❍ **C.** Just-in-time permissions
- ❍ **D.** Smart card with picture ID

.....

The Answer: D. Smart card with picture ID
A smart card commonly includes a certificate that can be used as a multifactor authentication of something you have. These smart cards are commonly combined with an employee identification card, and often require a separate PIN (Personal Identification Number) as an additional authentication factor.

The incorrect answers:
A. USB-connected storage drive with FDE
FDE (Full Disk Encryption) will protect the data on a drive, but it doesn't provide a factor of authentication.

B. Employee policy manual
Employee policy manuals aren't commonly associated with a specific individual, so they are not a good factor of authentication.

C. Just-in-time permissions
Just-in-time permissions provide a method of distributing login credentials on a temporary or as-needed basis. Just-in-time permissions may or may not include any type of multi-factor authentication.

More information:
SY0-701, Objective 4.6 - Multi-Factor Authentication
https://professormesser.link/701040603

C18. A company's network team has been asked to build an IPsec tunnel to a new business partner. Which of the following security risks would be the MOST important to consider?

- ❍ **A.** Supply chain attack
- ❍ **B.** Unsupported systems
- ❍ **C.** Business email compromise
- ❍ **D.** Typosquatting

.....

The Answer: A. Supply chain attack
A direct connection to a third-party creates potential access for an attacker. Most organizations will include a firewall to help monitor and protect against any supply chain attacks.

The incorrect answers:
B. Unsupported systems
Although unsupported systems can be a significant security concern, this question did not document any issues with outdated or legacy devices.

C. Business email compromise
Business email compromise uses an organization's existing email addresses as an attack destination. A business email compromise does not require an IPsec tunnel to a partner location.

D. Typosquatting
Typosquatting uses misspelled domain names in an effort to mislead a victim. This often takes the form of phishing emails or unauthorized website links. There are no domain name spelling issues associated with this new IPsec connection.

More information:
SY0-701, Objective 2.2 - Common Threat Vectors
https://professormesser.link/701020201

C19. A company's human resources team maintains a list of all employees participating in the corporate savings plan. A third-party financial company uses this information to manage stock investments for the employees. Which of the following would describe this financial company?

- ❍ **A.** Processor
- ❍ **B.** Owner
- ❍ **C.** Controller
- ❍ **D.** Custodian

.....

The Answer: A. Processor
A data processor performs some type of action to the data, and this is often a different group within the organization or a third-party company. In this example, the third-party financial organization is the data processor of the employee's financial data.

The incorrect answers:
B. Owner
The data owner is often an executive of the company and is ultimately responsible for the use and security of this data.

C. Controller
A data controller manages the data. In this example, the human resources team would control the access and use of the employee data.

D. Custodian
A data custodian is responsible for the accuracy, privacy, and security of the data. Many organizations will hire data custodians to ensure all data is properly protected and maintained.

More information:
SY0-701, Objective 5.1 - Data Roles and Responsibilities
https://professormesser.link/701050105

C20. A technology company is manufacturing a military-grade radar tracking system designed to identify any nearby unmanned aerial vehicles (UAVs). The UAV detector must be able to instantly identify and react to a vehicle without delay. Which of the following would BEST describe this tracking system?

- ❍ **A.** RTOS
- ❍ **B.** IoT
- ❍ **C.** ICS
- ❍ **D.** SDN

The Answer: A. RTOS
This tracking system requires an RTOS (Real-Time Operating System) to instantly react to input without any significant delays or queuing in the operating system. Operating systems used by the military, automobile manufacturers, and industrial equipment companies often use RTOS to process certain transactions without any significant delays.

The incorrect answers:
B. IoT
IoT (Internet of Things) devices are generally associated with home automation and do not have a requirement for real-time operation.

C. ICS
An ICS (Industrial Control System) is often a dedicated network used exclusively to manage and control manufacturing equipment, power generation equipment, water management systems, and other industrial machines. Although some industrial control systems may use an RTOS, using a real-time operating system is not a requirement of an ICS.

D. SDN
An SDN (Software Defined Network) splits the functions of a network device into separate planes of operation. These logical units extend the functionality and management of a single device and provide a method of easily deploying devices in the cloud.

More information:
SY0-701, Objective 3.1 - Other Infrastructure Concepts
https://professormesser.link/701030103

C21. An administrator is writing a script to convert an email message to a help desk ticket and assign the ticket to the correct department. Which of the following should be administrator use to complete this script?

- ❍ **A.** Role-based access controls
- ❍ **B.** Federation
- ❍ **C.** Due diligence
- ❍ **D.** Orchestration

.....

The Answer: D. Orchestration
Orchestration describes the process of automation, and is commonly associated with large scale automation or automating processes between different systems.

The incorrect answers:
A. Role-based access controls
Role-based access control is used to associate a job function with a set of rights and permissions. The scripting described in this question does not specifically require any role-based access controls.

B. Federation
Federation commonly describes the process of authenticating to one system using the credentials associated with another system. The scripting process in this question would not require federation.

C. Due diligence
Due diligence usually involves the investigation performed on a third party prior to doing business. An internal help desk script would not require any due diligence.

More information:
SY0-701, Objective 4.7 - Scripting and Automation
http://professormesser.link/701040701

C22. A security administrator would like a report showing how many attackers are attempting to use a known vulnerability to gain access to a corporate web server. Which of the following should be used to gather this information?

- ❍ **A.** Application log
- ❍ **B.** Metadata
- ❍ **C.** IPS log
- ❍ **D.** Windows log

The Answer: C. IPS log
An IPS (Intrusion Prevention System) commonly uses a database of known vulnerabilities to identify and block malicious network traffic. This log of attempted exploits would provide the required report information.

The incorrect answers:
A. Application log
An application log provides a summary of internal application functions and procedures. An application log would not commonly identify and log security events.

B. Metadata
Metadata is a summary of information attached to a file or document. Metadata does not commonly store security events and would not be a valid source for this reporting data.

D. Windows log
The Windows Event Viewer shows the logs for the applications, security, and other aspects of the Windows operating system. An operating system log would not commonly gather information on network-based attacks.

More information:
SY0-701, Objective 4.9 - Log Data
https://professormesser.link/701040901

C23. During a ransomware outbreak, an organization was forced to rebuild database servers from known good backup systems. In which of the following incident response phases were these database servers brought back online?

- ❍ **A.** Recovery
- ❍ **B.** Lessons learned
- ❍ **C.** Containment
- ❍ **D.** Detection

.....

The Answer: A. Recovery
The recovery phase focuses on getting things back to normal after an attack. This is the phase that removes malware, fixes vulnerabilities, and recovers the damaged systems.

The incorrect answers:
B. Lessons learned
Once an event is over, it's useful to have a post-incident meeting to discuss the things that worked and things that didn't.

C. Containment
When an event occurs, it's important to minimize the impact. Isolation and containment can help to limit the spread and effect of an event.

D. Detection
Detecting and identifying the event is an important step that initiates the rest of the incident response processes.

More information:
SY0-701, Objective 4.8 - Incident Response
https://professormesser.link/701040801

C24. A security administrator is installing a web server with a newly built operating system. Which of the following would be the best way to harden this OS?

- ❍ **A.** Create a backup schedule
- ❍ **B.** Install a device certificate
- ❍ **C.** Remove unnecessary software
- ❍ **D.** Disable power management features

.....

The Answer: C. Remove unnecessary software
The process of hardening an operating system makes it more difficult to attack. In this example, the only step that would limit the attack surface is to remove any unnecessary or unused software.

The incorrect answers:
A. Create a backup schedule
Although a backup schedule is an important security task, the process of performing backups doesn't make the system any more resistant to a potential attack.

B. Install a device certificate
A device certificate can be used to verify the ownership of a remote system. However, installing a device certificate does not make the remote system more resistant to an attack.

D. Disable power management features
Disabling the power management features of an operating system does not generally have any impact on the overall security of the system.

More information:
SY0-701, Objective 2.5 - Hardening Techniques
https://professormesser.link/701020503

C25. A network IPS has created this log entry:

```
Frame 4: 937 bytes on wire (7496 bits), 937 bytes captured
Ethernet II, Src: HewlettP_82:d8:31, Dst: Cisco_a1:b0:d1
Internet Protocol Version 4, Src: 172.16.22.7, Dst: 10.8.122.244
Transmission Control Protocol, Src Port: 3863, Dst Port: 1433
Application Data: SELECT * FROM users WHERE username='x'
     or 'x'='x' AND password='x' or 'x'='x'
```

Which of the following would describe this log entry?

- ❍ **A.** Phishing
- ❍ **B.** Brute force
- ❍ **C.** SQL injection
- ❍ **D.** Cross-site scripting

.....

The Answer: C. SQL injection
The SQL injection is contained in the application data. The attacker was attempting to circumvent the authentication through the use of equivalent SQL statements ('x'='x').

The incorrect answers:
A. Phishing
Phishing attempts use social engineering to gain access to private or sensitive information. This example does not appear to contain any private information.

B. Brute force
A brute force attempt would include many failed attempts at a password. This log does not appear to have any repeated password attempts.

D. Cross-site scripting
Cross-site scripting takes advantage of the trust a user has for a site. This example does not appear to take advantage of any previous authentication or trust.

More information:
SY0-701, Objective 2.3 - SQL Injection
https://professormesser.link/701020306

C26. An incident response team would like to validate their disaster recovery plans without making any changes to the infrastructure. Which of the following would be the best course of action?

- ❍ **A.** Tabletop exercise
- ❍ **B.** Hot site fail-over
- ❍ **C.** Simulation
- ❍ **D.** Penetration test

The Answer: A. Tabletop exercise
A tabletop exercise is a walk-through exercise where the disaster recovery process can be discussed in a conference room without making any changes to the existing systems.

The incorrect answers:
B. Hot site fail-over
A fail-over to a hot site would involve significant changes to the infrastructure, services, and operations teams.

C. Simulation
A simulation is a useful test of disaster recovery processes, but it often requires a change to the existing systems to properly test the simulated disaster.

D. Penetration test
A penetration test will identify vulnerabilities, but it will not provide any evaluation of the disaster recovery process or policies.

More information:
SY0-701, Objective 3.4 - Recovery Testing
https://professormesser.link/701030403

C27. A system administrator has installed a new firewall between the corporate user network and the data center network. When the firewall is turned on with the default settings, users complain the application in the data center is no longer working. Which of the following would be the BEST way to correct this application issue?

- ❍ **A.** Create a single firewall rule with an explicit deny
- ❍ **B.** Build a separate VLAN for the application
- ❍ **C.** Create firewall rules that match the application traffic flow
- ❍ **D.** Enable firewall threat blocking

.....

The Answer: C. Create firewall rules that match the application traffic flow

By default, most firewalls implicitly deny all traffic. Firewall rules must be built to match the traffic flows, and only then will traffic pass through the firewall.

The incorrect answers:

A. Create a single firewall rule with an explicit deny

By default, most firewalls have an implicit deny as the last policy in the firewall rules. If traffic does not match any other firewall rule, then the implicit deny drops the traffic. Manually configuring an explicit deny doesn't provide any additional traffic control because of the already-existing implicit deny, and it doesn't allow any traffic to pass through the firewall because the rule itself denies all traffic.

B. Build a separate VLAN for the application

VLAN (Virtual Local Area Network) separation can be used to manage traffic flows or provide additional security options, but creating a VLAN won't bypass an existing firewall deny rule.

D. Enable firewall threat blocking

Many next-generation firewalls can identify and block malicious network traffic in real-time. However, enabling this feature would not resolve any existing communication issues between the user network and the data center network.

More information:
SY0-701, Objective 4.5 - Firewalls
https://professormesser.link/701040501

C28. Which of these would be used to provide HA for a web-based database application?

- ❍ **A.** SIEM
- ❍ **B.** UPS
- ❍ **C.** DLP
- ❍ **D.** VPN concentrator

The Answer: B. UPS
HA (High Availability) means the service should always be on and available. The only device on this list providing HA is the UPS (Uninterruptible Power Supply). If power is lost, the UPS will provide electricity using battery power or a gas-powered generator.

The incorrect answers:
A. SIEM
A SIEM (Security Information and Event Management) system consolidates data from devices on the network and provides log searching and reporting features. A SIEM does not provide any HA functionality.

C. DLP
DLP (Data Loss Prevention) is a method of identifying and preventing the transfer of personal or confidential information through the network. DLP does not provide any HA functionality.

D. VPN concentrator
A VPN (Virtual Private Network) concentrator is used as an endpoint to an endpoint VPN solution. VPN concentrators do not provide any HA functionality.

More information:
SY0-701, Objective 3.4 - Power Resiliency
https://professormesser.link/701030405

C29. Each year, a certain number of laptops are lost or stolen and must be replaced by the company. Which of the following would describe the total cost the company spends each year on laptop replacements?

- ❍ **A.** SLE
- ❍ **B.** SLA
- ❍ **C.** ALE
- ❍ **D.** ARO

.....

The Answer: C. ALE
The ALE (Annual Loss Expectancy) is the total amount of the financial loss over an entire year.

The incorrect answers:
A. SLE
SLE (Single Loss Expectancy) describes the loss for a single incident.

B. SLA
SLA (Service Level Agreement) is a contractual agreement that specifies a minimum service level.

D. ARO
An ARO (Annualized Rate of Occurrence) is the number of times an event is expected to occur in a year.

More information:
SY0-701, Objective 5.2 - Risk Analysis
https://professormesser.link/701050202

C30. A network administrator is viewing a log file from a web server:

```
https://www.example.com/?s=/Index/think/
app/invokefunction&function=call_user_func_
array&vars[0]=md5&vars[1][0]=__HelloThinkPHP
```

Which of the following would be the BEST way to prevent this attack?

- ❍ **A.** Static code analyzer
- ❍ **B.** Input validation
- ❍ **C.** Allow list
- ❍ **D.** Secure cookies

The Answer: B. Input validation
In this example, the attacker is attempting to use a remote code execution exploit. Input validation can be used to create a very specific filter of allowed input, and a strict validation process would have prevented the web server from processing this attack information.

The incorrect answers:
A. Static code analyzer
A static code analyzer is useful when evaluating the security of existing source code. In this example, the input is dynamic and is initiated by the attacker.

C. Allow list
An allow list would limit user access to an application, but it would not limit the type of input from the users.

D. Secure cookies
Secure cookies ensure the information contained in the browser cookie is encrypted and only viewable by the end user. Secure cookies would not prevent a remote code execution attack.

More information:
SY0-701, Objective 4.1 - Application Security
https://professormesser.link/701040105

C31. Sam would like to send an email to Jack and have Jack verify that Sam was the sender of the email. Which of these should Sam use to provide this verification?

- ❍ **A.** Digitally sign with Sam's private key
- ❍ **B.** Digitally sign with Sam's public key
- ❍ **C.** Digitally sign with Jack's private key
- ❍ **D.** Digitally sign with Jack's public key

.....

The Answer: A. Digitally sign with Sam's private key
The sender of a message digitally signs with their own private key to ensure integrity, authentication, and non-repudiation of the signed contents. The digital signature is validated with the sender's public key.

The incorrect answers:
B. Digitally sign with Sam's public key
Since everyone effectively has access to all public keys, adding a digital signature with a publicly available key doesn't provide any security features.

C. Digitally sign with Jack's private key
Jack's private key would only be available to Jack, so Sam could not possibly use Jack's private key when performing any cryptographic functions.

D. Digitally sign with Jack's public key
Since Jack's public key would be available to anyone, using Jack's public key for a digital signature would not provide any security features.

More information:
SY0-701, Objective 1.4 - Hashing and Digital Signatures
https://professormesser.link/701010406

C32. The contract of a long-term temporary employee is ending. Which of these would be the MOST important part of the off-boarding process?

- ❍ **A.** Perform an on-demand audit of the user's privileges
- ❍ **B.** Archive the decryption keys associated with the user account
- ❍ **C.** Document the user's outstanding tasks
- ❍ **D.** Obtain a signed copy of the Acceptable Use Policies

The Answer: B. Archive the decryption keys associated with the user account

Without the decryption keys, it will be impossible to access any of the user's protected files once they leave the company. Given the other possible answers, this one is the only one that would result in unrecoverable data loss if not properly followed.

The incorrect answers:

A. Perform an on-demand audit of the user's privileges
The user's account will be disabled once they leave the organization, so an audit of their privileges would not be very useful.

C. Document the user's outstanding tasks
Creating documentation is important, but it's not as important as retaining the user's data with the decryption keys.

D. Obtain a signed copy of the Acceptable Use Policies
Acceptable Use Policies (AUPs) are usually signed during the on-boarding process. You won't need an AUP if the user is no longer accessing the network.

More information:
SY0-701, Objective 5.1 - Security Procedures
https://professormesser.link/701050103

C33. A cybersecurity analyst has been asked to respond to a denial of service attack against a web server, and the analyst has collected the log files and data from the server. Which of the following would allow a future analyst to verify the data as original and unaltered?

- ❍ **A.** E-discovery
- ❍ **B.** Root cause analysis
- ❍ **C.** Legal hold
- ❍ **D.** Data hashing

.....

The Answer: D. Data hashing
Data hashing creates a unique message digest based on stored data. If the data is tampered with, a hash taken after the change will differ from the original value. This allows the forensic engineer to identify if information has been changed. .

The incorrect answers:
A. E-discovery
E-Discovery (Electronic Discovery) describes the collection, preparation, review, interpretation, and production of electronic documents. Collecting information through e-discovery does not guarantee the integrity of the data.

B. Root cause analysis
A root cause analysis examines the evidence and determines the reason for the breach or attack. Performing a root cause analysis can help prevent future attacks, but it would not ensure the integrity of the collected data.

C. Legal hold
A legal hold is a legal technique to preserve relevant information. This legal hold will ensure the data remains accessible for any legal preparation that needs to occur prior to litigation.

More information:
SY0-701, Objective 4.8 - Digital Forensics
https://professormesser.link/701040803

C34. A security administrator is reviewing authentication logs. The logs show a large number of accounts with at least three failed authentication attempts during the previous week. Which of the following would BEST explain this report data?

- ❍ **A.** Downgrade attack
- ❍ **B.** Phishing
- ❍ **C.** Injection
- ❍ **D.** Spraying

The Answer: D. Spraying
A spraying attack attempts to discover login credentials using a small number of authentication attempts. If the password isn't discovered in those few attempts, the brute force process stops before any account lockouts occur. An attacker could potentially perform a spraying attack across many accounts without any noticeable alerts or alarms.

The incorrect answers:
A. Downgrade attack
A downgrade attack takes advantage of a cryptographic weakness or vulnerability to gain access. This weakness is often due to an unpatched application or a poorly implemented cryptographic process. In this example, the attack is focused on a small number of brute force attempts and not on a cryptographic issue.

B. Phishing
Phishing is a useful attack for gathering information. Since a phishing attack often gathers valid authentication details, it's not necessary for the phishing process to also perform a brute force attack.

C. Injection
An injection attack adds additional information to a data stream in an attempt to access systems or data which would normally not be accessible. An injection attack does not generally perform a brute force attack.

More information:
SY0-701, Objective 2.4 - Password Attacks
https://professormesser.link/701020414

C35. A security administrator has been asked to block all browsing to casino gaming websites. Which of the following would be the BEST way to implement this requirement?

- ❍ **A.** Tune the IPS signatures
- ❍ **B.** Block port tcp/443 on the firewall
- ❍ **C.** Configure 802.1X for web browsing
- ❍ **D.** Add a content filter rule

.....

The Answer: D. Add a content filter rule
Web filters contain a large database of categorized website addresses, and this allows an administrator to create rules to block browsing attempts to specific content. For example, a content filter may allow browsing to news and business sites, but block browsing attempts to gaming and shopping sites.

The incorrect answers:
A. Tune the IPS signatures
An IPS (Intrusion Prevention System) can identify and block known exploits within network traffic. An IPS does not maintain a categorized list of websites, and tuning the IPS signatures would not block specific website categories.

B. Block port tcp/443 on the firewall
Blocking a single port would not provide filtering on a specific website category. In this example, blocking all tcp/443 traffic would effectively block all web browsing traffic to secure sites.

C. Configure 802.1X for web browsing
802.1X is an authentication protocol often used with network access control. The 802.1X protocol does not provide any filtering or categorization of website traffic.

More information:
SY0-701, Objective 4.5 - Web Filtering
https://professormesser.link/701040502

C36. A company is experiencing downtime and outages when application patches and updates are deployed during the week. Which of the following would help to resolve these issues?

- ❍ **A.** Onboarding considerations
- ❍ **B.** Incident response policies
- ❍ **C.** Change management procedures
- ❍ **D.** Decentralized governance

.....

The Answer: C. Change management procedures
Change management defines a series of best practices for implementing changes in a complex technical environment. The goals of change management are to implement updates and changes while also maintaining the uptime and availability of critical business systems.

The incorrect answers:
A. Onboarding considerations
The onboarding process occurs when new employees join the organization. A change to the onboarding process would not correct the outages created by patches and updates.

B. Incident response policies
An operating system update or application patch is not categorized as a security incident, so updating or modifying an incident response process would not have any effect on system availability.

D. Decentralized governance
In this example, the governance of a system does not appear to be effective in managing changes, and decentralizing the governance would not commonly provide any resolution for unmanaged changes.

More information:
SY0-701, Objective 1.3 - Change Management Process
https://professormesser.link/701010301

C37. A company is implementing a series of steps to follow when responding to a security event. Which of the following would provide this set of processes and procedures?

- ❍ **A.** MDM
- ❍ **B.** DLP
- ❍ **C.** Playbook
- ❍ **D.** Zero trust

.....

The Answer: C. Playbook
A playbook provides a conditional set of steps to follow when addressing a specific event. An organization might have separate playbooks for investigating a data breach, responding to a virus infection, or recovering from a ransomware attack.

The incorrect answers:
A. MDM
An MDM (Mobile Device Management) service provides configuration and control of remote devices. An MDM does not provide a checklist for handling security events.

B. DLP
DLP (Data Loss Prevention) is a security solution for identifying and blocking the transfer of sensitive information across the network. A DLP would not provide steps to follow during a security event.

D. Zero trust
Zero trust is a security philosophy which considers all devices to be untrusted. Inherent trust and trusted connections between devices are not part of a zero trust model. Zero trust does not provide checklists for security tasks.

More information:
SY0-701, Objective 5.1 - Security Procedures
https://professormesser.link/701050103

C38. A transportation company maintains a scheduling application and a database in a virtualized cloud-based environment. Which of the following would be the BEST way to backup these services?

- ❍ **A.** Journaling
- ❍ **B.** Snapshot
- ❍ **C.** RTOS
- ❍ **D.** Containerization

.....

The Answer: B. Snapshot
Virtual machines (VMs) have a snapshot feature to capture both a full backup of the virtual system and incremental changes that occur over time. It's common to take a snapshot of a VM for backup purposes or before making any significant changes to the VM. If the changes need to be rolled back, a previous snapshot can be selected and instantly applied to the VM.

The incorrect answers:
A. Journaling
Journaling protects the integrity of a file system or database by writing information to a journal before making any changes to the primary data source. This allows the system to recover from a potential fault and prevent file corruption.

C. RTOS
An RTOS (Real-Time Operating System) has a deterministic processing schedule and is often associated with time-sensitive applications. An RTOS is not a backup mechanism.

D. Containerization
Containerization describes an application deployment strategy where a single file or container includes everything required to run an application. Containerization itself is not a backup mechanism.

More information:
SY0-701, Objective 3.4 - Backups
https://professormesser.link/701030404

C39. In an environment using discretionary access controls, which of these would control the rights and permissions associated with a file or directory?

- ❍ **A.** Administrator
- ❍ **B.** Owner
- ❍ **C.** Group
- ❍ **D.** System

The Answer: B. Owner
The owner of an object controls access in a discretionary access control model. The object and type of access is at the discretion of the owner, and they can determine who can access the file and the type of access they would have.

The incorrect answers:
A. Administrator
Administrators generally label objects when using mandatory access control, but they are not involved with discretionary access control.

C. Group
Assigning rights and permissions to a group and then assigning users to the group are common when using role-based access control.

D. System
The system does not determine individual user rights and permissions when using discretionary access control.

More information:
SY0-701, Objective 4.6 - Access Controls
https://professormesser.link/701040602

C40. A security administrator has installed a network-based DLP solution to determine if file transfers contain PII. Which of the following describes the data during the file transfer?

- ❍ **A.** In-use
- ❍ **B.** In-transit
- ❍ **C.** Highly available
- ❍ **D.** At-rest

The Answer: B. In-transit
Data in-transit describes information actively moving across the network. As the information passes through switches and routers, it is considered to be in-transit.

The incorrect answers:
A. In-use
Data in-use is in the memory of a system and is accessible to an application.

C. Highly available
High availability (HA) is usually associated with redundancy or fault-tolerance. Data moving through the network would not be considered highly available.

D. At-rest
Data at-rest resides on a storage device.

More information:
SY0-701, Objective 3.3 - States of Data
https://professormesser.link/701030302

C41. A medical imaging company would like to connect all remote locations together with high speed network links. The network connections must maintain high throughput rates and must always be available during working hours. In which of the following should these requirements be enforced with the network provider?

- ❍ **A.** Service level agreement
- ❍ **B.** Memorandum of understanding
- ❍ **C.** Non-disclosure agreement
- ❍ **D.** Acceptable use policy

The Answer: A. Service level agreement
A service level agreement (SLA) is used to contractually define the minimum terms for services. In this example, the medical imaging company would require an SLA from the network provider for the necessary throughput and uptime metrics.

The incorrect answers:
B. Memorandum of understanding
A memorandum of understanding (MOU) is an informal letter of intent. The MOU is not a signed contract, and there are no contractual obligations associated with the content of an MOU.

C. Non-disclosure agreement
A non-disclosure agreement (NDA) is used between entities to prevent the use and dissemination of confidential information.

D. Acceptable use policy
An acceptable use policy (AUP) commonly details the rules of behavior for employees using an organization's network and computing resources.

More information:
SY0-701, Objective 5.3 - Agreement Types
https://professormesser.link/701050302

C42. A company is implementing a security awareness program for their user community. Which of the following should be included for additional user guidance and training?

- ❍ **A.** Daily firewall exception reporting
- ❍ **B.** Information on proper password management
- ❍ **C.** Periodic vulnerability scanning of external services
- ❍ **D.** Adjustments to annualized loss expectancy

.....

The Answer: B. Information on proper password management
User awareness programs focus on security fundamentals that everyone in the organization can use during their normal work day. Protecting and managing passwords is an important security consideration for all users in the company.

The incorrect answers:
A. Daily firewall exception reporting
Daily security reports can provide important insight into the organization's security posture, but it doesn't provide security guidance for the user community.

C. Periodic vulnerability scanning of external services
Periodic audits and security scans can provide validation and identify potential issues, but the vulnerability scan results don't provide any help to the user community with their ongoing security responsibilities.

D. Adjustments to annualized loss expectancy
Annualized loss expectancy estimates can be important for budgeting and security planning, but those expenses aren't related to user community guidance and training.

More information:
SY0-701, Objective 5.6 - User Training
https://professormesser.link/701050602

C43. A security administrator is preparing a phishing email as part of a periodic employee security awareness campaign. The email is spoofed to appear as an unknown third-party and asks employees to immediately click a link or their state licensing will be revoked. Which of the following should be the expected response from the users?

- ❍ **A.** Delete the message
- ❍ **B.** Click the link and make a note of the URL
- ❍ **C.** Forward the message to others in the department
- ❍ **D.** Report the suspicious link to the help desk

.....

The Answer: D. Report the suspicious link to the help desk
The users should be trained to report anything suspicious, and unusual links in an email message would certainly be an important security concern.

The incorrect answers:
A. Delete the message
Deleting the email would avoid any interaction with the malicious link, but it wouldn't provide any additional security for others in the organization. The contents of the email might also provide important information for removing similar messages and blocking future emails.

B. Click the link and make a note of the URL
The links inside of email messages are inherently insecure, and a best practice is to never click unknown or unexpected links or attachments inside of email messages.

C. Forward the message to others in the department
Forwarding a message with potentially malicious links would be a significant security concern, and it would be more secure to forward a copy to the IT security team.

More information:
SY0-701, Objective 5.6 - Security Awareness
https://professormesser.link/701050601

C44. A security administrator would like to minimize the number of certificate status checks made by web site clients to the certificate authority. Which of the following would be the BEST option for this requirement?

- ❍ **A.** OCSP stapling
- ❍ **B.** Self-signed certificates
- ❍ **C.** CRL
- ❍ **D.** Wildcards

The Answer: A. OCSP stapling
OCSP (Online Certificate Status Protocol) stapling allows the certificate holder verify their own certificate status. The OCSP status is commonly "stapled" into the SSL/TLS handshake process. Instead of contacting the certificate authority to verify the certificate, the verification is included with the initial network connection to the server.

The incorrect answers:
B. Self-signed certificates
Self-signed certificates could be created for internal company use, but this would not change the process for validating the status of a certificate.

C. CRL
A CRL (Certificate Revocation List) is a list of revoked certificates maintained by the certificate authority. To view the CRL, an end-user client would directly access the CA.

D. Wildcards
Wildcards are added to certificates for use across multiple devices. Wildcards would not decrease the number of certificate status checks for a particular service.

More information:
SY0-701, Objective 1.4 - Certificates
https://professormesser.link/701010408

C45. A company is concerned their EDR solution will not be able to stop more advanced ransomware variants. Technicians have created a backup and restore utility to get most systems up and running less than an hour after an attack. What type of security control is associated with this restore process?

- ❍ **A.** Directive
- ❍ **B.** Compensating
- ❍ **C.** Preventive
- ❍ **D.** Detective

.....

The Answer: B. Compensating
Instead of preventing an attack, a compensating control is used to restore systems using other means. A streamlined backup and restore process compensates for the limited security features of the EDR (Endpoint Detection and Response) software.

The incorrect answers:
A. Directive
Directive controls define policies and processes, but directive controls won't provide a method for recovering from a ransomware infection.

C. Preventive
A preventive control will block access. The EDR software on a workstation is an example of a preventive control.

D. Detective
A detective control may not be able to block an attack, but it can identify and alert if an attack is underway.

More information:
SY0-701, Objective 1.1 - Security Controls
https://professormesser.link/701010101

C46. To upgrade an internal application, the development team provides the operations team with instructions for backing up, patching the application, and reverting the patch if needed. The operations team schedules a date for the upgrade, informs the business divisions, and tests the upgrade process after completion. Which of the following describes this process?

- ❍ **A.** Code signing
- ❍ **B.** Continuity planning
- ❍ **C.** Usage auditing
- ❍ **D.** Change management

The Answer: D. Change management
Change management is the process for making any type of change, such as a software upgrade, a hardware replacement, or any other type of modification to the existing environment. Having a formal change management process minimizes the risk of a change and makes everyone aware of the changes as they occur.

The incorrect answers:
A. Code signing
Application developers often digitally sign their software to ensure no modifications are made before the software is installed. The code signing process does not provide any guidance for an organization's internal processes associated with installing updated software.

B. Continuity planning
Continuity planning focuses on keeping the business running when a disruption occurs. Disaster recovery planning is a type of continuity plan.

C. Usage auditing
Usage auditing determines how resources are used. For example, a system administrator may perform a usage audit to determine which resources are used with a particular application or service.

More information:
SY0-701, Objective 1.3 - Change Management Process
https://professormesser.link/701010301

C47. A company is implementing a public file-storage and cloud-based sharing service, and would like users to authenticate with an existing account on a trusted third-party web site. Which of the following should the company implement?

- ❍ **A.** SSO
- ❍ **B.** Federation
- ❍ **C.** Least privilege
- ❍ **D.** Discretionary access controls

.....

The Answer: B. Federation
Federation provides authentication and authorization between two entities using a separate trusted authentication platform. For example, a web site could allow authentication using an existing account on a third-party social media site.

The incorrect answers:
A. SSO
SSO (Single Sign-On) does not inherently require authentication to be processed by a third-party. SSO allows a user to authenticate one time to gain access to all assigned resources. No additional authentication is required after the initial SSO login process is complete.

C. Least privilege
Least privilege ensures users only receive the permissions necessary to perform their assigned functions. Least privilege is not used to authenticate users to a third-party site.

D. Discretionary access controls
Discretionary access controls are used by a data owner to allow or prevent access to the data. Discretionary access controls are not used to authenticate users to a third-party database.

More information:
SY0-701, Objective 4.6 - Identity and Access Management
https://professormesser.link/701040601

C48. A system administrator is viewing this output from a file integrity monitoring report:

```
15:43:01 - Repairing corrupted file C:\Windows\System32\kernel32.dll
15:43:03 - Repairing corrupted file C:\Windows\System32\netapi32.dll
15:43:07 - Repairing corrupted file C:\Windows\System32\user32.dll
15:43:43 - Repair complete
```

Which of the following malware types is the MOST likely cause of this output?

- ❍ **A.** Ransomware
- ❍ **B.** Logic bomb
- ❍ **C.** Rootkit
- ❍ **D.** Keylogger

.....

The Answer: C. Rootkit
A rootkit modifies operating system files to become part of the core OS. The kernel, user, and networking libraries in Windows are core operating system files.

The incorrect answers:
A. Ransomware
Ransomware commonly presents itself as a warning message on the user's screen, and most aspects of the operating system would be disabled. Ransomware also encrypts user documents and would not easily be repaired by replacing system files.

B. Logic bomb
A logic bomb waits for a predefined event to begin operation. Logic bombs do not commonly modify core operating system files.

D. Keylogger
A keylogger does not commonly embed itself in core operating system files. Keyloggers often run as an independent process and compile logs and keystrokes to send across the network to the attacker.

More information:
SY0-701, Objective 2.4 - Other Malware Types
https://professormesser.link/701020404

C49. What type of vulnerability would be associated with this log information?

```
GET http://example.com/show.asp?view=../../Windows/
    system.ini HTTP/1.1
```

- ❍ **A.** Buffer overflow
- ❍ **B.** Directory traversal
- ❍ **C.** DoS
- ❍ **D.** Cross-site scripting

.....

The Answer: B. Directory traversal
Directory traversal attempts to read or access files outside the scope of the web server's file directory. The pair of dots in a file path (..) refers to the parent directory, so this example is attempt to move back two parent directories before proceeding into the /Windows directory. In a properly configured web server, this traversal should not be possible.

The incorrect answers:
A. Buffer overflow
A buffer overflow would attempt to store information into an area of memory that overflows the boundary of the buffer. The information in the log does not show any overflow attempt.

C. DoS
A DoS (Denial of Service) is designed to make a system or service unavailable. Although running any unknown command can be unpredictable, it would be unusual for these commands to cause any downtime.

D. Cross-site scripting
A cross-site scripting attack would normally include a script referencing another site trusted by the browser. In this example, the commands appear to be related to the existing URL and not a third-party site.

More information:
SY0-701, Objective 2.4 - Application Attacks
https://professormesser.link/701020412

C50. A developer has created an application to store password information in a database. Which of the following BEST describes a way of protecting these credentials by adding random data to the password?

- ❍ **A.** Hashing
- ❍ **B.** Data masking
- ❍ **C.** Salting
- ❍ **D.** Asymmetric encryption

The Answer: C. Salting
Passwords are often stored as hashes, but the hashes themselves are often subject to brute force or rainbow table attacks. It's common to add some additional random data (a salt) to a password before the hashing process. This ensures that each password is truly random when stored, and it makes it more difficult for an attacker to discover all of the stored passwords.

The incorrect answers:
A. Hashing
Hashing is a one-way cryptographic function which takes an input, such as a password, and creates a fixed size string of random information. The process of adding additional information to the original data before the hashing process is called salting.

B. Data masking
Data masking hides data from human eyes. For example, instead of showing a credit card number, the data mask will show asterisks in all but the last four digits.

D. Asymmetric encryption
Asymmetric encryption is an encryption method which uses one key for encryption and a different key for decryption. Asymmetric encryption does not add additional random information to a hash.

More information:
SY0-701, Objective 3.3 - Protecting Data
https://professormesser.link/701030303

C51. Which of the following processes provides ongoing building and testing of newly written code?

- ❍ **A.** Continuous integration
- ❍ **B.** Continuity of operations
- ❍ **C.** Version control
- ❍ **D.** Race condition

The Answer: A. Continuous integration
With continuous integration, code can be constantly written and merged into the central repository many times each day.

The incorrect answers:
B. Continuity of operations
Continuity of operations is used during disaster recovery or incident recovery. This process provides options for keeping the business processes available during or after the incident.

C. Version control
Version control is used to track changes to a file or configuration information over time. This allows changes to be applied and, if necessary, easily reverted to a previous version.

D. Race condition
A race condition is caused when two related processes occur simultaneously without knowledge of each other. A race condition is not related the process of building or testing code.

More information:
SY0-701, Objective 4.7 - Scripting and Automation
https://professormesser.link/701040701

C52. Which of the following BEST describes a responsibility matrix?

- ❍ **A.** A visual summary of cloud provider accountability
- ❍ **B.** Identification of tasks at each step of a project plan
- ❍ **C.** A list of cybersecurity requirements based on the identified risks
- ❍ **D.** Ongoing group discussions regarding cybersecurity

.....

The Answer: A. A visual summary of cloud provider accountability
A cloud provider commonly creates a responsibility matrix to document the service coverage between the cloud provider and the customer. For example, a cloud responsibility matrix may show the cloud provider responsible for network controls and the customer responsible for all stored data.

The incorrect answers:
B. Identification of tasks at each step of a project plan
A project plan will include many tasks, and the list of tasks is often shown as part of the overall project plan or in a summarized chart.

C. A list of cybersecurity requirements based on the identified risks
Risk assessment provides a security administrator with the information needed to build proper security controls for the documented risks.

D. Ongoing group discussions regarding cybersecurity
Risk assessment can involve constant monitoring and analysis of current trends, risks, and response options. This information can be gathered from group discussions, expert presentations, and security conferences and programs.

More information:
SY0-701, Objective 3.1 - Cloud Infrastructures
https://professormesser.link/701030101

C53. A security administrator is implementing an authentication system for the company. Which of the following would be the best choice for validating login credentials for all usernames and passwords in the authentication system?

- ❍ **A.** CA
- ❍ **B.** SIEM
- ❍ **C.** LDAP
- ❍ **D.** WAF

.....

The Answer: C. LDAP
LDAP (Lightweight Directory Access Protocol) is a common standard for authentication. LDAP is an open standard and is available across many different operating systems and devices.

The incorrect answers:
A. CA
A CA (Certificate Authority) is a trusted service for certificate creation and management. The CA itself is not responsible for validating login credentials.

B. SIEM
A SIEM (Security and Information Management) service consolidates log files from diverse systems and can create reports based on the correlation of this data. A SIEM is not part of the authentication process.

D. WAF
A WAF (Web Application Firewall) is used to protect a web-based application from exploits and other attacks. A WAF is not used to validate login credentials.

More information:
SY0-701, Objective 4.6 - Identity and Access Management
https://professormesser.link/701040601

C54. A technician is reviewing this information from an IPS log:

```
MAIN_IPS: 22June2023 09:02:50 reject 10.1.111.7
Alert: HTTP Suspicious Webdav OPTIONS Method Request; Host: Server
Severity: medium; Performance Impact:3;
Category: info-leak; Packet capture; disable
Proto:tcp; dst:192.168.11.1; src:10.1.111.7
```

Which of the following can be associated with this log information? (Select TWO)

- ❍ **A.** The attacker sent a non-authenticated BGP packet to trigger the IPS
- ❍ **B.** The source of the attack is 192.168.11.1
- ❍ **C.** The event was logged but no packets were dropped
- ❍ **D.** The source of the attack is 10.1.111.7
- ❍ **E.** The attacker sent an unusual HTTP packet to trigger the IPS

The Answer: D. The source of the attack is 10.1.111.7 and
E. The attacker sent an unusual HTTP packet to trigger the IPS
The second line of the IPS log shows the type of alert, and this record indicates a suspicious HTTP packet was sent. The last line of the IPS log shows the protocol, destination, and source IP address information. The source IP address is 10.1.111.7.

The incorrect answers:
A. The attacker sent a non-authenticated BGP packet to trigger the IPS
The alert for this IPS log does not indicate any non-authenticated packets or BGP packets.

B. The source of the attack is 192.168.11.1
The last line of the log identifies the protocol and IP addresses. The "src" address is the source of the packet and is identified as 10.1.111.7.

C. The event was logged but no packets were dropped
The first line of the log shows the name of the IPS which identified the issue, the date and time, and disposition. In this log entry, the packet was rejected from IP address 10.1.111.7.

More information:
SY0-701, Objective 4.9 - Log Data
https://professormesser.link/701040901

C55. A company has contracted with a third-party to provide penetration testing services. The service includes a port scan of each externally-facing device. This is an example of:

- ❍ **A.** Initial exploitation
- ❍ **B.** Privilege escalation
- ❍ **C.** Known environment
- ❍ **D.** Active reconnaissance

.....

The Answer: D. Active reconnaissance
Active reconnaissance sends traffic across the network, and this traffic can be viewed and logged. Performing a port scan will send network traffic to a server, and most port scan attempts can be identified and logged by an IPS (Intrusion Prevention System).

The incorrect answers:
A. Initial exploitation
An exploit attempt is common when performing a penetration test, but a port scan is not exploiting any vulnerabilities.

B. Privilege escalation
If a penetration test is able to exploit a system and obtain a higher level of rights and permissions, then the test is successful at escalating the access privileges. A port scan does not gain access to a system, and it will not provide any privilege escalation.

C. Known environment
A known environment fully documents the network and systems within the scope of a penetration test. In this example, there's no mention of testing environment documentation provided to the penetration testers.

More information:
SY0-701, Objective 5.5 - Penetration Tests
https://professormesser.link/701050502

C56. An access point in a corporate headquarters office has the following configuration:

```
IP address: 10.1.10.1
Subnet mask: 255.255.255.0
DHCPv4 Server: Enabled
SSID: Wireless
Wireless Mode: 802.11n
Security Mode: WEP-PSK
Frequency band: 2.4 GHz
Software revision: 2.1
MAC Address: 60:3D:26:71:FF:AA
IPv4 Firewall: Enabled
```

Which of the following would apply to this configuration?

❍ **A.** Invalid frequency band

❍ **B.** Weak encryption

❍ **C.** Incorrect IP address and subnet mask

❍ **D.** Invalid software version

The Answer: B. Weak encryption
A common issue is weak or outdated security configurations. Older encryptions such as DES and WEP should be updated to use newer and stronger encryption technologies.

The incorrect answers:
A. Invalid frequency band
The 2.4 GHz frequency band is a valid frequency range for 802.11n networks.

C. Incorrect IP address and subnet mask
None of the listed configuration settings show any issues with the IP address or subnet mask.

D. Invalid software version
The software version of the access point does not have any configuration options and would not be considered invalid.

More information:
SY0-701, Objective 2.2 - Common Threat Vectors
https://professormesser.link/701020201

C57. An attacker has gained access to an application through the use of packet captures. Which of the following would be MOST likely used by the attacker?

- ❍ **A.** Overflow
- ❍ **B.** Forgery
- ❍ **C.** Replay
- ❍ **D.** Injection

The Answer: C. Replay
A replay attack uses previously transmitted information to gain access to an application or service. This information is commonly captured in network packets and replayed to the service.

The incorrect answers:
A. Overflow
A buffer overflow attack attempts to store a large number into a smaller sized memory space. This can sometimes improperly change the value of memory areas that are outside of the smaller space.

B. Forgery
A cross-site request forgery commonly uses malicious links to take advantage of the trust a site might have for a user's browser. Packet captures are not necessary to perform a forgery attack.

D. Injection
The unwanted injection of data into a database, library, or any other data flow is an injection attack. The information contained in a packet capture is not commonly used during an injection attack.

More information:
SY0-701, Objective 2.4 - Replay Attacks
https://professormesser.link/701020410

C58. A company is receiving complaints of slowness and disconnections to their Internet-facing web server. A network administrator monitors the Internet link and finds excessive bandwidth utilization from thousands of different IP addresses. Which of the following would be the MOST likely reason for these performance issues?

- ❍ **A.** DDoS
- ❍ **B.** DNS spoofing
- ❍ **C.** RFID cloning
- ❍ **D.** Wireless jamming

The Answer: A. DDoS
A DDoS (Distributed Denial of Service) is the failure of a service caused by many different remote devices. In this example, the DDoS is related to a bandwidth utilization exhaustion caused by excessive server requests.

The incorrect answers:
B. DNS spoofing
DNS (Domain Name System) spoofing modifies DNS information on a DNS server or a client to direct users to an unauthorized site. DNS spoofing would not be the cause for these performance issues.

C. RFID cloning
RFID (Radio Frequency Identification) cloning is used to duplicate an existing RFID device. These devices are not commonly associated with network communication to a public web server.

D. Wireless jamming
Wireless jamming disrupts wireless networks and prevents any type of communication. The communication issues to a public web server would not be associated with wireless networking.

More information:
SY0-701, Objective 2.4 - Denial of Service
https://professormesser.link/701020406

C59. A company has created an itemized list of tasks to be completed by a third-party service provider. After the services are complete, this document will be used to validate the completion of the services. Which of the following would describe this agreement type?

- ❍ **A.** SLA
- ❍ **B.** SOW
- ❍ **C.** NDA
- ❍ **D.** BPA

.....

The Answer: B. SOW
A SOW (Statement of Work) is a detailed list of tasks, items, or processes to be completed by a third-party. The SOW lists the job scope, location, deliverables, and any other specifics associated with the agreement. The SOW is also used as a checklist to verify the job was completed properly by the service provider.

The incorrect answers:
A. SLA
An SLA (Service Level Agreement) sets the minimum terms of service between a customer and a service provider. This agreement often contains terms for expected uptime, response time requirements, and other minimum service levels required by the customer.

C. NDA
An NDA (Non-Disclosure Agreement) is a confidentiality agreement between parties. The agreement is designed to protect information such as trade secrets, business activities, or anything else included in the NDA. An NDA does not generally contain an itemized list of service requests.

D. BPA
A BPA (Business Partners Agreement) is used between entities going into business together. A list of itemized service requests would not be part of a BPA.

More information:
SY0-701, Objective 5.3 - Agreement Types
https://professormesser.link/701050302

C60. A company is deploying a series of internal applications to different cloud providers. Which of the following connection types should be deployed for this configuration?

- ❍ **A.** Air-gapped
- ❍ **B.** 802.1X
- ❍ **C.** Site-to-site IPsec VPN
- ❍ **D.** Jump server
- ❍ **E.** SD-WAN

.....

The Answer: E. SD-WAN
An SD-WAN (Software Defined Networking in a Wide Area Network) network allows users to efficiently communicate directly to cloud-based applications.

The incorrect answers:
A. Air-gapped
An air-gapped network would be physically isolated from other networks. In this question, connectivity is required between the users and the various cloud providers.

B. 802.1X
802.1X is a standard for port-based network access control and would most likely be used when a user first connects to the network and before a user would connect to the Internet.

C. Site-to-site IPsec VPN
Although it's physically possible to connect every site to every other site (or to cloud providers), it's difficult to scale this design to larger environments. This connectivity also becomes difficult to manage as applications move from one cloud provider site to another.

D. Jump server
A jump server is often used to allow external access to internal devices, commonly for maintenance or administrative tasks. A jump server is not a router and does not forward traffic between users and cloud-based applications.

More information:
SY0-701, Objective 3.2 - Secure Communication
https://professormesser.link/701030207

C61. A company is updating components within the control plane of their zero-trust implementation. Which of the following would be part of this update?

- ❍ **A.** Policy engine
- ❍ **B.** Subjects
- ❍ **C.** Policy enforcement point
- ❍ **D.** Zone configurations

.....

The Answer: A. Policy engine
The policy engine is located in the control plane and evaluates each access decision based on security policy and other information sources. The policy engine determines if access should be granted, denied, or revoked.

The incorrect answers:
B. Subjects
Subjects use the zero-trust data plane, and are often end-users, applications, or other non-human entities.

C. Policy enforcement point
A policy enforcement point resides in the data plane and is the gatekeeper for allowing, monitoring, and terminating connections.

D. Zone configurations
Zero-trust uses security zones to easily apply access policies, and these zones operate in the data plane.

More information:
SY0-701, Objective 1.2 - Zero Trust
https://professormesser.link/701010205

C62. Which of the following malware types would cause a workstation to participate in a DDoS?

- ❍ **A.** Bot
- ❍ **B.** Logic bomb
- ❍ **C.** Ransomware
- ❍ **D.** Keylogger

The Answer: A. Bot
A bot (robot) is malware that installs itself on a system and then waits for instructions. It's common for botnets to use thousands of bots to perform DDoS (Distributed Denial of Service) attacks.

The incorrect answers:
B. Logic bomb
A logic bomb waits for a predefined event to occur. The scope of devices infected with a logic bomb are relatively small and localized as compared to a botnet.

C. Ransomware
Ransomware locks a system and prevents it from operating. The locked device does not commonly participate in a DDoS.

D. Keylogger
A keylogger will silently capture keystrokes and transmit an archive of those keystrokes to a third-party. A keylogger does not commonly participate in a DDoS.

More information:
SY0-701, Objective 2.4 - Denial of Service
https://professormesser.link/701020406

C63. Which of these are used to force the preservation of data for later use in court?

- ❍ **A.** Chain of custody
- ❍ **B.** Data loss prevention
- ❍ **C.** Legal hold
- ❍ **D.** E-discovery

The Answer: C. Legal hold
A legal hold is a legal technique to preserve relevant information. This process will ensure the data remains accessible for any legal preparation prior to litigation.

The incorrect answers:
A. Chain of custody
Chain of custody ensures the integrity of evidence is maintained. The contents of the evidence are documented, and each person who contacts the evidence is required to document their activity.

B. Data loss prevention
Data loss prevention (DLP) is a technique for identifying sensitive information transmitted across the network, such as Social Security numbers, credit card numbers, and other PII (Personally Identifiable Information). DLP is not a legal technique.

D. E-discovery
E-discovery describes the process of identifying and collecting electronic documents and media. The e-discovery process itself does not force the preservation of data.

More information:
SY0-701, Objective 4.8 - Digital Forensics
https://professormesser.link/701040803

C64. A company would like to automatically monitor and report on any movement occurring in an open field at the data center. Which of the following would be the BEST choice for this task?

- ❍ **A.** Bollard
- ❍ **B.** Microwave sensor
- ❍ **C.** Access control vestibule
- ❍ **D.** Fencing

The Answer: B. Microwave sensor
Microwave sensors can detect movement across large areas such as open fields.

The incorrect answers:
A. Bollard
A bollard is a barricade used to prevent access. Bollards often allow people to pass through a specific access point, but limit access for cars and other vehicles.

C. Access control vestibule
An access control vestibule is a room designed to manage the flow of people through the area. It's common to see access control vestibules used as an entry point to a data center or secure facility.

D. Fencing
Fencing can create a perimeter to prevent access to a large open field, but it wouldn't detect or alert on any type of movement.

More information:
SY0-701, Objective 1.2 - Physical Security
https://professormesser.link/701010206

C65. A company is releasing a new product, and part of the release includes the installation of load balancers to the public web site. Which of the following would best describe this process?

- ❍ **A.** Platform diversity
- ❍ **B.** Capacity planning
- ❍ **C.** Multi-cloud systems
- ❍ **D.** Permission restrictions

.....

The Answer: B. Capacity planning
Capacity planning describes the process of matching the supply of a resource to the demand. In this example, the company is planning for an increased interest in their products and are increasing the overall capacity of their web server resources.

The incorrect answers:
A. Platform diversity
Platform diversity describes the use of different platforms to provide a similar service. For example, a company may decide to use both Linux and Windows platforms for their web services. In this question, the platform used by the web services is not mentioned.

C. Multi-cloud systems
Multi-cloud systems will use more than a single cloud provider to provide a service. In this question, there were no specific references to cloud providers.

D. Permission restrictions
Permission restrictions would limit access to data or resources, and the addition of multiple identical servers would not indicate a change to the existing permissions.

More information:
SY0-701, Objective 3.4 - Capacity Planning
https://professormesser.link/701030402

C66. A system administrator would like to prove an email message was sent by a specific person. Which of the following describes the verification of this message source?

- ❍ **A.** Non-repudiation
- ❍ **B.** Key escrow
- ❍ **C.** Asymmetric encryption
- ❍ **D.** Steganography

The Answer: A. Non-repudiation
Non-repudiation is used to verify the source of data or a message. Digital signatures are commonly used for non-repudiation.

The incorrect answers:
B. Key escrow
Key escrow describes a third-party responsible for holding or managing keys or certificates. Key escrow does not provide verification of a data source.

C. Asymmetric encryption
Asymmetric encryption describes data encryption using one key and the decryption of this data with a different key. The use of asymmetric encryption by itself does not provide proof of origin.

D. Steganography
Steganography describes hiding one type of data within another media type. For example, hiding encrypted data within an image is a form of steganography. Steganography does not provide proof of origin.

More information:
SY0-701, Objective 1.2 - Non-repudiation
https://professormesser.link/701010202

C67. A security administrator has created a policy to alert if a user modifies the hosts file on their system. Which of the following behaviors does this policy address?

- ❍ **A.** Unexpected
- ❍ **B.** Self-assessment
- ❍ **C.** Unintentional
- ❍ **D.** Risky

The Answer: D. Risky
Making a change to the hosts file can be a security concern, and many systems will prevent this change without elevated permissions. Modifying the hosts file would be categorized as risky behavior.

The incorrect answers:
A. Unexpected
Editing a hosts file is a specific task with an intentional result. The user modification of the hosts file would not generally be considered an unexpected event.

B. Self-assessment
A self-assessment is often used in internal audits to informally gather information about potential security risks. A self-assessment is not part of a user's intentional file edits.

C. Unintentional
A user editing a file is an active process and is often associated with performing a specific configuration change or task.

More information:
SY0-701, Objective 5.6 - Security Awareness
https://professormesser.link/701050601

C68. A company has identified a web server data breach resulting in the theft of financial records from 150 million customers. A security update to the company's web server software was available for two months prior to the breach. Which of the following would have prevented this breach from occurring?

- ❍ **A.** Patch management
- ❍ **B.** Full disk encryption
- ❍ **C.** Disabling unnecessary services
- ❍ **D.** Application allow lists

The Answer: A. Patch management
This question describes an actual breach which occurred in 2017 to web servers at a large credit bureau. This breach resulted in the release of almost 150 million customer names, Social Security numbers, addresses, and birth dates. A web server vulnerability announced in March of 2017 was left unpatched, and attackers exploited the vulnerability two months later. The attackers were in the credit bureau network for 76 days before they were discovered. A formal patch management process would have clearly identified this vulnerability and would have given the credit bureau the opportunity to mitigate or patch the vulnerability well before it would have been exploited.

The incorrect answers:
B. Full disk encryption
Full disk encryption (FDE) would prevent unauthenticated access to the data, but the web server would be an authorized user and would have normal access to the areas of the operating system necessary for normal operation. Enabling FDE would not provide any additional security against a data breach.

C. Disable unnecessary services
It's always a good best practice to disable unnecessary services, but this breach attacked a very necessary web service.

D. Application allow lists
Application allow lists would prevent unauthorized applications from running, but it would not prevent an attack to the web service application.

More information:
SY0-701, Objective 2.5 - Mitigation Techniques
https://professormesser.link/701020502

C69. During the onboarding process, the IT department requires a list of software applications associated with the new employee's job functions. Which of the following would describe the use of this information?

- ❍ **A.** Access control configuration
- ❍ **B.** Encryption settings
- ❍ **C.** Physical security requirements
- ❍ **D.** Change management

.....

The Answer: A. Access control configuration
The onboarding team needs to assign the proper access controls to new employees, and the list of applications provides additional details regarding application and data access.

The incorrect answers:
B. Encryption settings
A list of applications required by a new employee does not generally have any impact on the encryption settings used by these applications.

C. Physical security requirements
Physical security requirements would not generally be based on the list of required applications for a new employee. Most physical security requirements are determined by the organization's IT security team.

D. Change management
Adding rights and permissions for a new user would be a normal procedure and would not require a formal change management process.

More information:
SY0-701, Objective 5.1 - Security Standards
https://professormesser.link/701050102

C70. A system administrator has identified an unexpected username on a database server, and the user has been transferring database files to an external server over the company's Internet connection. The administrator then performed these tasks:

- Physically disconnected the Ethernet cable on the database server
- Disabled the unknown account
- Configured a firewall rule to prevent file transfers from the server

Which of the following would BEST describe this part of the incident response process?

❍ **A.** Eradication
❍ **B.** Containment
❍ **C.** Lessons learned
❍ **D.** Preparation

.....

The Answer: B. Containment
The containment phase isolates events which can quickly spread and get out of hand. A file transfer from a database server can quickly be contained by disabling any ability to continue the file transfer.

The incorrect answers:
A. Eradication
Eradication focuses on removing the cause of the event and restoring the systems back to their non-compromised state.

C. Lessons learned
After the event is over, the lessons learned phase helps everyone learn and improve the process for the next event.

D. Preparation
Before an event occurs, it's important to have the contact numbers, tools, and processes ready to go.

More information:
SY0-701, Objective 4.8 - Incident Response
https://professormesser.link/701040801

C71. Which of the following would be the MOST effective use of asymmetric encryption?

- ❍ **A.** Real-time video encryption
- ❍ **B.** Securely store passwords
- ❍ **C.** Protect data on mobile devices
- ❍ **D.** Create a shared session key

The Answer: D. Create a shared session key
The Diffie-Hellman algorithm can combine public and private keys to derive the same session key. This allows two devices to create and use this shared session key without sending the key across the network.

The incorrect answers:
A. Real-time video encryption
The high speeds required for real-time video encryption and decryption would not be an efficient use case for asymmetric encryption. High-speed or large-scale encryption commonly uses a faster method of encryption and decryption.

B. Securely store passwords
The best practice for password storage is to use hashes instead of encryption. Hashes ensure a stored password can't be reverse engineered to produce the original password.

C. Protect data on mobile devices
The limited CPU and power available on a mobile device requires a more efficient form of confidentiality than asymmetric encryption. For example, it's common for mobile devices to use elliptic curve cryptography (ECC).

More information:
SY0-701, Objective 1.4 - Key Exchange
https://professormesser.link/701010403

C72. Each salesperson in a company receives a laptop with applications and data to support their sales efforts. The IT manager would like to prevent third-parties from gaining access to this information if the laptop is stolen. Which of the following would be the BEST way to protect this data?

- ❍ **A.** Remote wipe
- ❍ **B.** Full disk encryption
- ❍ **C.** Biometrics
- ❍ **D.** VPN

.....

The Answer: B. Full disk encryption
With full disk encryption, everything written to the laptop's local drive is stored as encrypted data. If the laptop was stolen, the thief would not have the credentials to decrypt the drive data.

The incorrect answers:
A. Remote wipe
Although a remote wipe function is useful, it's a reactive response and does not provide any data protection prior to erasing the data.

C. Biometrics
Biometric authentication can limit access to the operating system, but the laptop's storage drive can still be removed and accessed from another computer.

D. VPN
A VPN (Virtual Private Network) would encrypt all data transferred over the network, but it would not protect any stored data if the laptop was stolen.

More information:
SY0-701, Objective 1.4 - Encrypting Data
https://professormesser.link/701010402

C73. A security administrator has compiled a list of all information stored and managed by an organization. Which of the following would best describe this list?

- ❍ **A.** Sanitization
- ❍ **B.** Metadata
- ❍ **C.** Known environment
- ❍ **D.** Data inventory

.....

The Answer: D. Data inventory
A data inventory describes a list of all data managed by an organization. This inventory includes the owner, update frequency, and format of the data.

The incorrect answers:
A. Sanitization
Data sanitization involves the complete removal of data without any method of recovery. Data sanitization is often used when clearing storage media for reuse or disposal.

B. Metadata
Metadata is data which describes other data sources. Email header information, network headers, and file characteristics are common examples of metadata.

C. Known environment
A known environment commonly describes the information provided to a penetration tester. A known environment provides a complete overview of the in-scope devices associated with a penetration test.

More information:
SY0-701, Objective 5.4 - Privacy
https://professormesser.link/701050402

C74. A security administrator would like to monitor all outbound Internet connections for malicious software. Which of the following would provide this functionality?

- ❍ **A.** Jump server
- ❍ **B.** IPsec tunnel
- ❍ **C.** Forward proxy
- ❍ **D.** Load balancer

The Answer: C. Forward proxy
A proxy server can be used to monitor incoming and outgoing network communication. Proxy servers can be used to identify malicious software, filter content, or increase performance through file caching.

The incorrect answers:
A. Jump server
A jump server is commonly used to provide administrative access to a secure network connection. Jump servers are not used to monitor or filter Internet connections.

B. IPsec tunnel
An IPsec tunnel is associated with an encrypted connection between devices or sites. An IPsec tunnel would not be used to monitor or manage network content or Internet connections.

D. Load balancer
Load balancers are used to increase capacity by separating the processing load between multiple servers. Load balancers are not used for network monitoring or security filtering.

More information:
SY0-701, Objective 3.2 - Network Appliances
https://professormesser.link/701030203

C75. What type of security control would be associated with corporate security policies?

- ❍ **A.** Technical
- ❍ **B.** Operational
- ❍ **C.** Managerial
- ❍ **D.** Physical

The Answer: C. Managerial
A managerial control type is associated with security design and implementation. Security policies and standard operating procedures are common examples of a managerial control type.

The incorrect answers:
A. Technical
Technical security controls are implemented using systems, such as operating system controls, firewalls, or anti-virus software.

B. Operational
Operational controls are implemented by people instead of systems. An example of an operational security control type would be security guards or awareness programs.

D. Physical
A physical control type would limit physical access. For example, a door lock or badge reader would be a physical control.

More information:
SY0-701, Objective 1.1 - Security Controls
https://professormesser.link/701010101

C76. Which of the following would be the MOST significant security concern when protecting against organized crime?

- ❍ **A.** Prevent users from posting passwords near their workstations
- ❍ **B.** Require identification cards for all employees and guests
- ❍ **C.** Maintain reliable backup data
- ❍ **D.** Use access control vestibules at all data center locations

The Answer: C. Maintain reliable backup data
A common objective for organized crime is an organization's data, and attacks from organized crime can sometimes encrypt or delete data. A good set of backups can often resolve these issues quickly and without any ransomware payments to an organized crime syndicate.

The incorrect answers:
A. Prevent users from posting passwords near their workstations
Organized crime members usually access systems remotely. Although it's important for users to protect their passwords, the organized crime members aren't generally in a position to view information on a person's desk.

B. Require identification cards for all employees and guests
Since the criminal syndicate members rarely visit a site, having identification for employees and visitors isn't the most significant concern associated with this threat actor.

D. Use access control vestibules at all data center locations
Access control vestibules control the flow of people through an area. Organized crime members aren't usually visiting a company's data center.

More information:
SY0-701, Objective 2.1 - Threat Actors
https://professormesser.link/701020101

C77. An application team has been provided with a hardened version of Linux to use with a new application installation, and this includes installing a web service and the application code on the server. Which of the following would BEST protect the application from attacks?

- ❍ **A.** Build a backup server for the application
- ❍ **B.** Run the application in a cloud-based environment
- ❍ **C.** Implement a secure configuration of the web service
- ❍ **D.** Send application logs to the SIEM via syslog

.....

The Answer: C. Implement a secure configuration of the web service
The tech support resources for many services will include a list of hardening recommendations. This hardening may include account restrictions, file permission settings, internal service configuration options, and other settings to ensure that the service is as secure as possible.

The incorrect answers:
A. Build a backup server for the application
Of course, you should always have a backup. Although the backup may help recover quickly from an attack, the backup itself won't protect the application from attacks.

B. Run the application in a cloud-based environment
The location of the application service won't provide any significant protection against attacks. Given the options available, running the application in the cloud would not be the best option available.

D. Send application logs to the SIEM via syslog
It's always useful to have a consolidated set of logs, but the logs on the SIEM (Security Information and Event Management) server won't protect the application from attacks.

More information:
SY0-701, Objective 2.5 - Hardening Techniques
https://professormesser.link/701020503

C78. A system administrator has configured MAC filtering on their corporate access point, but access logs show unauthorized users accessing the network. Which of the following should the administrator configure to prevent future unauthorized use?

- ❍ **A.** Enable WPA3 encryption
- ❍ **B.** Remove unauthorized MAC addresses from the filter
- ❍ **C.** Modify the SSID name
- ❍ **D.** Modify the channel frequencies

.....

The Answer: A. Enable WPA3 encryption
A MAC (Media Access Control) address can be spoofed on a remote device, which means anyone within the vicinity of the access point can view and use legitimate MAC addresses. To ensure proper authentication, the system administrator can enable WPA3 (Wi-Fi Protected Access version 3) with a pre-shared key or 802.1X can be used to integrate with an existing authentication database.

The incorrect answers:
B. Remove unauthorized MAC addresses from the filter
Since MAC addresses are visible when capturing packets, any unauthorized users affected by the removal of a MAC address would simply view the remaining MAC addresses in use and spoof those addresses to gain access.

C. Modify the SSID name
The SSID (Service Set Identifier) is the name associated with the wireless network. The name of the access point is not a security feature, so changing the name would not provide any additional access control.

D. Modify the channel frequencies
The frequencies used by the access point are chosen to minimize interference with other nearby wireless devices. These wireless channels are not security features and changing the frequency would not limit unauthorized access.

More information:
SY0-701, Objective 4.1 - Wireless Security Settings
https://professormesser.link/701040104

C79. A system administrator has been tasked with performing an application upgrade, but the upgrade has been delayed due to a different scheduled installation of an outdated device driver. Which of the following issues would best describe this change management delay?

- ❍ **A.** Deny list
- ❍ **B.** Legacy application
- ❍ **C.** Dependency
- ❍ **D.** Restricted activity

.....

The Answer: C. Dependency
Modifying one part of a system may first require changes to other components. In this example, the application upgrade is dependent on an updated version of a device driver.

The incorrect answers:
A. Deny list
A deny list would prevent an application from executing. In this question, an older version of the application is currently working, and there's no mention of preventing a newer version of the application from also working properly.

B. Legacy application
A legacy application is usually not supported by the developer, and it would be unusual for a legacy application to release an updated version of software.

D. Restricted activity
Most change control processes have a limited scope, and a technician would be restricted from making changes outside of that scope. In this example, the device driver and the application are both part of the change control process, but one of the changes must occur before the other change can be made.

More information:
SY0-701, Objective 1.3 - Technical Change Management
https://professormesser.link/701010302

C80. During an initial network connection, a supplicant communicates to an authenticator, which then sends an authentication request to an Active Directory database. Which of the following would BEST describe this authentication technology?

- ❍ **A.** Federation
- ❍ **B.** UTM
- ❍ **C.** 802.1X
- ❍ **D.** PKI

The Answer: C. 802.1X
IEEE 802.1X is a standard for port-based network access control (NAC). When 802.1X is enabled, devices connecting to the network do not gain access until they provide the correct authentication credentials. This 802.1X standard refers to the client as the supplicant, the switch is commonly configured as the authenticator, and the back-end authentication server is often a centralized user database.

The incorrect answers:
A. Federation
Federation would allow members of one organization to authenticate to the network of another organization using their normal credentials.

B. UTM
A UTM (Unified Threat Management) system is a legacy all-in-one security device which combines a firewall, anti-virus, content filtering, and other security features into a single system.

D. PKI
PKI (Public Key Infrastructure) is a method of describing the public-key encryption technologies and its supporting policies and procedures. PKI does not require the use of supplicants, authenticators, or authentication servers.

More information:
SY0-701, Objective 3.2 - Port Security
https://professormesser.link/701030204

C81. A security researcher has been notified of a potential hardware vulnerability. Which of the following should the researcher evaluate as a potential security issue?

- ❍ **A.** Firmware versions
- ❍ **B.** Firewall configuration
- ❍ **C.** SQL requests
- ❍ **D.** XSS attachments

.....

The Answer: A. Firmware versions
Firmware describes the software inside of a hardware device and is often used as the operating system of the hardware. Issues with hardware vulnerabilities are usually resolved by updating firmware in the vulnerable system.

The incorrect answers:
B. Firewall configuration
Misconfigured firewall software could certainly be a security issue, but the problem reported in this question is specific to a hardware vulnerability.

C. SQL requests
A SQL (Structured Query Language) request is commonly associated with a database-related process. SQL requests are software-related and are not related to a hardware vulnerability.

D. XSS attachments
XSS (Cross-site Scripting) is an exploit which uses the trust in a browser to gain access to a web site. An XSS attachment describes a malicious script included in an email or similar delivery mechanism. Cross-site scripting is a software exploit and is not associated with a hardware vulnerability.

More information:
SY0-701, Objective 2.3 - Hardware Vulnerabilities
https://professormesser.link/701020308

C82. Visitors to a corporate data center must enter through the main doors of the building. Which of the following security controls would be the BEST choice to successfully guide people to the front door? (Select TWO)

- ❍ **A.** Infrared sensors
- ❍ **B.** Bollards
- ❍ **C.** Biometrics
- ❍ **D.** Fencing
- ❍ **E.** Access badges
- ❍ **F.** Video surveillance

The Answers: B. Bollards and **D.** Fencing
Both bollards and fencing provide physical security controls to direct people to an area by limiting their access to other areas.

The incorrect answers:
A. Infrared sensors
Infrared sensors are able to detect infrared radiation in both dark and light environments. Infrared sensors are often included with surveillance video systems, but they wouldn't be used to direct individuals to the main doors of a building.

C. Biometrics
Biometrics provide a unique authentication factor, but they aren't commonly used to direct people to a particular building entrance.

E. Access Badges
Access badges are often used as both identification and access cards to secure areas of a facility. An access badge would not direct individuals to the main doors of a building.

F. Video surveillance
Video surveillance would make it easy to monitor and view visitors approaching the building, but it would not provide any directions to the front doors.

More information:
SY0-701, Objective 1.2 - Physical Security
https://professormesser.link/701010206

C83. A company's employees are required to authenticate each time a file share, printer, or SAN imaging system is accessed. Which of the following should be used to minimize the number of employee authentication requests?

- ❍ **A.** SSO
- ❍ **B.** OSINT
- ❍ **C.** MFA
- ❍ **D.** SCAP

.....

The Answer: A. SSO
SSO (Single Sign-On) accepts valid authentication requests and allows users to access multiple resources without requiring additional user authentications.

The incorrect answers:
B. OSINT
OSINT (Open Source Intelligence) is information gathered from publicly available sources such as social media sites, online forums, and other data sources. OSINT is not associated with user authentication.

C. MFA
MFA (Multi-factor authentication) is used to provide additional proof of a user's identity during the authentication process. MFA is not used to minimize the number of authentication requests required by a system.

D. SCAP
SCAP (Security Content Automation Protocol) is a standard method used by security tools to identify and act on the same criteria. SCAP is not used to minimize the number of required authentications.

More information:
SY0-701, Objective 4.6 - Identity and Access Management
https://professormesser.link/701040601

C84. A company has recently moved from one accounting system to another, and the new system includes integration with many other divisions of the organization. Which of the following would ensure that the correct access has been provided to the proper employees in each division?

- ❍ **A.** Geolocation
- ❍ **B.** Onboarding process
- ❍ **C.** Account de-provisioning
- ❍ **D.** Internal self-assessment

The Answer: D. Internal self-assessment
An internal self-assessment with audit can verify users have the correct permissions and all users meet the practice of least privilege.

The incorrect answers:
A. Geolocation
Geolocation would allow the system to assign rights and permissions based on physical location. In this question, there's no documentation on where users are located and how those locations could be used for access control.

B. Onboarding process
The onboarding process is used when a new person is hired or transferred into the organization. In this example, none of the users were identified as new employees.

C. Account de-provisioning
Account de-provisioning is the disabling of an account and archiving of user information. This process usually occurs when an employee has left the organization.

More information:
SY0-701, Objective 5.5 - Audits and Assessments
https://professormesser.link/701050501

C85. An attacker has circumvented a web-based application to send commands directly to a database. Which of the following would describe this attack type?

- ❍ **A.** Downgrade
- ❍ **B.** SQL injection
- ❍ **C.** Cross-site scripting
- ❍ **D.** On-path

.....

The Answer: B. SQL injection
A SQL (Structured Query Language) injection takes advantage of poorly written web applications. These web applications do not properly restrict the user input, and the resulting attack bypasses the application and "injects" SQL commands directly into the database itself.

The incorrect answers:
A. Downgrade
A downgrade attack commonly takes advantage of a poorly implemented cryptographic functions to force an application to use sub-optimal or non-existent security features.

C. Cross-site scripting
A cross-site scripting attack commonly uses scripts to execute commands on a third-party website. These types of attacks take advantage of the trust of a local browser, but they don't commonly have direct access to a database.

D. On-path
An on-path attack is often used to capture, monitor, or inject information into an existing data flow. An on-path attack is not commonly used for SQL injection attacks.

More information:
SY0-701, Objective 2.3 - SQL Injection
https://professormesser.link/701020306

C86. A group of business partners is using blockchain technology to monitor and track raw materials and parts as they are transferred between companies. Where would a partner find these tracking details?

- ❍ **A.** Ledger
- ❍ **B.** HSM
- ❍ **C.** SIEM
- ❍ **D.** HIPS

The Answer: A. Ledger
The ledger is a shared document with a list of all blockchain transactions. The ledger is shared among everyone in the blockchain, and all transactions are available to view on this central ledger.

The incorrect answers:
B. HSM
An HSM (Hardware Security Module) provides secure key storage and cryptographic functions for servers and applications. An HSM does not provide tracking services.

C. SIEM
A SIEM (Security Information and Event Manager) is commonly used to consolidate log files and create reports. A SIEM is not used to monitor blockchain transactions.

D. HIPS
A HIPS (Host-based Intrusion Prevention System) is used to identify exploit attempts on a device. A host-based IPS is not used to monitor data in a blockchain.

More information:
SY0-601, Objective 1.4 - Blockchain Technology
https://professormesser.link/701010407

C87. A network technician at a bank has noticed a significant decrease in traffic to the bank's public website. After additional investigation, the technician finds that users are being directed to a web site which looks similar to the bank's site but is not under the bank's control. Flushing the local DNS cache and changing the DNS entry does not have any effect. Which of the following has most likely occurred?

- ❍ **A.** DDoS
- ❍ **B.** Disassociation attack
- ❍ **C.** Buffer overflow
- ❍ **D.** Domain hijacking

The Answer: D. Domain hijacking
Domain hijacking will modify the primary DNS (Domain Name System) settings for a domain and allow an attacker to direct users to an IP address controlled by the attacker.

The incorrect answers:
A. DDoS
A DDoS (Distributed Denial of Service) would prevent users from accessing a service. In this example, users were accessing an unauthorized service.

B. Disassociation attack
A disassociation attack is a wireless vulnerability which can remove devices from a wireless network.

C. Buffer overflow
A buffer overflow is an application attack where an input of data can overwrite a buffer of memory space. A buffer overflow would not be used to redirect users to a different web page.

More information:
SY0-701, Objective 2.4 - DNS Attacks
https://professormesser.link/701020407

C88. A company runs two separate applications in their data center. The security administrator has been tasked with preventing all communication between these applications. Which of the following would be the BEST way to implement this security requirement?

- ❍ **A.** Firewall
- ❍ **B.** SDN
- ❍ **C.** Air gap
- ❍ **D.** VLANs

.....

The Answer: C. Air gap
An air gap is a physical separation between networks. Air gapped networks are commonly used to separate networks that must never communicate to each other.

The incorrect answers:
A. Firewall
A firewall would provide a method of filtering traffic between networks, but firewalls can often be misconfigured and inadvertently allow some traffic to pass. Although this is one option, it's not the best option given the option of an air gap.

B. SDN
SDN (Software Defined Networking) splits the functions of a networking device into separate logical units. SDN does not describe a security filter or firewall between applications in a data center.

D. VLANs
A VLAN (Virtual Local Area Network) is a logical method of segmenting traffic within network switches. Although this segmentation is effective, it's not as secure as an air gap.

More information:
SY0-701, Objective 3.1 - Network Infrastructure Concepts
https://professormesser.link/701030102

C89. A receptionist at a manufacturing company recently received an email from the CEO asking for a copy of the internal corporate employee directory. It was later determined that the email address was not sent from the CEO and the domain associated with the email address was not a corporate domain name. What type of training could help identify this type of attack in the future?

- ❍ **A.** Recognizing social engineering
- ❍ **B.** Proper password management
- ❍ **C.** Securing remote work environments
- ❍ **D.** Understanding insider threats

The Answer: A. Recognizing social engineering
Impersonating the CEO is a common social engineering technique. There are many ways to recognize a social engineering attack, and it's important to train everyone to spot these situations when they are occurring.

The incorrect answers:
B. Proper password management
Proper password management focuses on protecting passwords through the use of standard policies. These policies focus on topics such as password length, complexity, or password reuse.

C. Securing remote work environments
A remote work environment is very different to secure than a traditional work environment, but those concerns would not help to identify this type of social engineering attack.

D. Understanding insider threats
Although the attacker wasn't identified, we could assume that an employee would already have access to the internal corporate employee directory.

More information:
SY0-701, Objective 5.6 - User Training
https://professormesser.link/701050602

C90. Which of the following deployment models would a company follow if they require individuals to use their personal phones for work purposes?

- ❍ **A.** CYOD
- ❍ **B.** MDM
- ❍ **C.** BYOD
- ❍ **D.** COPE

The Answer: C. BYOD
BYOD (Bring Your Own Device) is a model where the employee owns the mobile device but can also use the same device for work.

The incorrect answers:
A. CYOD
The CYOD (Choose Your Own Device) model requires the corporation to purchase and own the device, but the user can select the device they would prefer to use.

B. MDM
An MDM (Mobile Device Manager) is used to manage company-owned and user-owned mobile devices.

D. COPE
COPE (Corporately Owned, Personally Enabled) devices are purchased by the company and deployed to the users. The organization keeps full control of the device and may allow the recipient to use the device for both business and personal use.

More information:
SY0-701, Objective 4.1 - Securing Wireless and Mobile
https://professormesser.link/701040103