CompTIA.SY0-701.vNov-2024.by.Jany.127q

Number: SY0-701
Passing Score: 800
Time Limit: 120
File Version: 13.0

Exam Code: SY0-701
Exam Name: CompTIA Security+

Exam A

QUESTION 1
An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?

A. Partially known environment
B. Unknown environment
C. Integrated
D. Known environment

Correct Answer: A
Section:
Explanation:
A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test.A partially known environment is also called a gray box test1.

QUESTION 2
A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

A. SPF
B. GPO
C. NAC
D. FIM

Correct Answer: D
Section:
Explanation:
FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.
Some of the benefits of FIM are:
It can prevent data tampering and corruption by verifying the checksums or hashes of the files.
It can identify the source and time of the changes by logging the user and system actions.
It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.
It can support forensic analysis and incident response by providing evidence and audit trails of the changes.
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section 5.3: Security Tools, p. 209-210
CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools, Objective 2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective: File integrity monitor, p. 12

QUESTION 3
Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation
B. Recovery

C. Lessons learned
D. Analysis

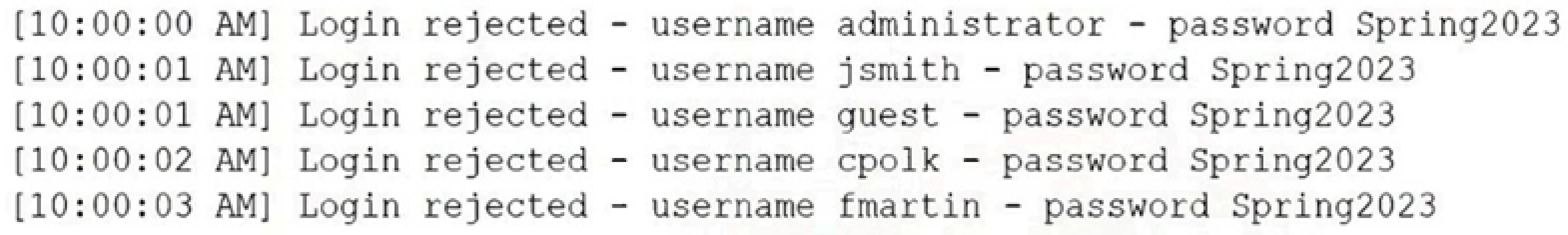
Correct Answer: A
Section:
Explanation:
Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.
Some of the activities that a security analyst performs during the preparation phase are:
Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.
Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.
Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.
Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.
Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.
Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.
Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4: Secure Systems Design, p. 279-280
CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

QUESTION 4
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

A. Jailbreaking
B. Memory injection
C. Resource reuse
D. Side loading

Correct Answer: D
Section:
Explanation:
Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices.Reference=Sideloading - CompTIA Security + Video Training | Interface Technical Training,Security+ (Plus) Certification | CompTIA IT Certifications,Load Balancers -- CompTIA Security+ SY0-501 -- 2.1,CompTIA Security+ SY0-601 Certification Study Guide.

QUESTION 5
A security analyst is reviewing the following logs:



```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A. Password spraying

B. Account forgery
C. Pass-t he-hash
D. Brute-force

Correct Answer: A
Section:
Explanation:
Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information.It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords12.
The logs show that the attacker is using the same password ('password123') to attempt to log in to different accounts ('admin', 'user1', 'user2', etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying.The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication3.
Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.
Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network.Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session4. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.
Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found.Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts5.The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server.Reference=1:Password spraying: An overview of password spraying attacks ... - Norton,2:Security: Credential Stuffing vs. Password Spraying - Baeldung,3:Brute Force Attack: A definition + 6 types to know | Norton,4:What is a Pass-the-Hash Attack? - CrowdStrike,5:What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet

QUESTION 6
An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

A. Secured zones
B. Subject role
C. Adaptive identity
D. Threat scope reduction

Correct Answer: D
Section:
Explanation:
The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.
One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access. This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.
The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions. Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.
Reference= https://bing.com/search?q=Zero+Trust+data+plane
https://learn.microsoft.com/en-us/security/zero-trust/deploy/data

QUESTION 7
A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

A. Certification

B. Inventory list

C. Classification

D. Proof of ownership

Correct Answer: A
Section:
Explanation:
The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery.A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel involved.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

QUESTION 8
Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

A. Compensating control

B. Network segmentation

C. Transfer of risk

D. SNMP traps

Correct Answer: A
Section:
Explanation:
A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers.Reference=Security Controls -- SY0-601 CompTIA Security+ : 5.1,Security Controls -- CompTIA Security+ SY0-501 -- 5.7,CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

QUESTION 9
The management team notices that new accounts that are set up manually do not always have correct access or permissions.
Which of the following automation techniques should a systems administrator use to streamline account creation?

A. Guard rail script

B. Ticketing workflow

C. Escalation script

D. User provisioning script

Correct Answer: D
Section:
Explanation:
A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions.A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources12.
The other options are not automation techniques that can streamline account creation:
Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network.A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software3.
Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers.A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process4.

Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage.
Reference=1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning -- CompTIA Security+ SY0-701 -- 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104. : CompTIA Security+ SY0-701 Certification Study Guide, page 105.

QUESTION 10
Which of the following involves an attempt to take advantage of database misconfigurations?

A. Buffer overflow
B. SQL injection
C. VM escape
D. Memory injection

Correct Answer: B
Section:
Explanation:
SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server.SQL injection can compromise the confidentiality, integrity, and availability of the data and the system.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2151

QUESTION 11
An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

A. Segmentation
B. Isolation
C. Patching
D. Encryption

Correct Answer: A
Section:
Explanation:
Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability.To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-3091

QUESTION 12
Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE
B. CVSS
C. CIA
D. CERT

Correct Answer: B
Section:
Explanation:
CVSS stands for Common Vulnerability Scoring System, which is a framework that provides a standardized way to assess and communicate the severity and risk of vulnerabilities. CVSS uses a set of metrics and formulas to calculate a numerical score ranging from 0 to 10, where higher scores indicate higher criticality. CVSS can help organizations prioritize remediation efforts and compare vulnerabilities across different systems and vendors.The

other options are not used to measure the criticality of a vulnerability, but rather to identify, classify, or report them.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 39

QUESTION 13
A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

A. Default credentials
B. Non-segmented network
C. Supply chain vendor
D. Vulnerable software

Correct Answer: C
Section:
Explanation:
A supply chain vendor is a third-party entity that provides goods or services to an organization, such as a SaaS provider. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices, breaches, or compromises that could affect the confidentiality, integrity, or availability of the system or its data. The organization should perform due diligence and establish a service level agreement with the vendor to mitigate this risk. The other options are not specific to the scenario of using a SaaS provider, but rather general risks that could apply to any system.

QUESTION 14
Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

A. Integrity
B. Availability
C. Confidentiality
D. Non-repudiation

Correct Answer: C
Section:
Explanation:
Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure. The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data. Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare. Integrity, availability, and non-repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

QUESTION 15
A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

A. Corrective
B. Preventive
C. Detective
D. Deterrent

Correct Answer: C
Section:
Explanation:

A detective control is a type of control that monitors and analyzes the events and activities in a system or a network, and alerts or reports when an incident or a violation occurs. A SIEM (Security Information and Event Management) system is a tool that collects, correlates, and analyzes the logs from various sources, such as firewalls, routers, servers, or applications, and provides a centralized view of the security status and incidents. An analyst who reviews the logs on a weekly basis can identify and investigate any anomalies, trends, or patterns that indicate a potential threat or a breach. A detective control can help the company to respond quickly and effectively to the incidents, and to improve its security posture and resilience.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 23. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.3, page 14.

QUESTION 16
An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?

A. Real-time recovery
B. Hot
C. Cold
D. Warm

Correct Answer: C
Section:
Explanation:
A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster.Reference=CompTIA Security+ SY0-701 Certification Study Guide, page 387;Backup Types -- SY0-601 CompTIA Security+ : 2.5, video at 4:50.

QUESTION 17
A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following best describes this policy?

A. Enumeration
B. Sanitization
C. Destruction
D. Inventory

Correct Answer: B
Section:
Explanation:
Sanitization is the process of removing sensitive data from a storage device or a system before it is disposed of or reused. Sanitization can be done by using software tools or hardware devices that overwrite the data with random patterns or zeros, making it unrecoverable. Sanitization is different from destruction, which is the physical damage of the storage device to render it unusable. Sanitization is also different from enumeration, which is the identification of network resources or devices, and inventory, which is the tracking of assets and their locations. The policy of securely wiping hard drives before sending decommissioned systems to recycling is an example of sanitization, as it ensures that no confidential data can be retrieved from the recycled devices.Reference=Secure Data Destruction -- SY0-601 CompTIA Security+ : 2.7, video at 1:00;CompTIA Security+ SY0-701 Certification Study Guide, page 387.

QUESTION 18
A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

A. Private
B. Critical
C. Sensitive
D. Public

Correct Answer: C

Section:
Explanation:
Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.
Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.
Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.
Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.
Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.
Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.
Reference=CompTIA Security+ SY0-701 Certification Study Guide, page 90-91;Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

QUESTION 19
A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

A. Local data protection regulations
B. Risks from hackers residing in other countries
C. Impacts to existing contractual obligations
D. Time zone differences in log correlation

Correct Answer: A
Section:
Explanation:
Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States. A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage. Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269. CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

QUESTION 20
Which of the following would be the best way to block unknown programs from executing?

A. Access control list
B. Application allow list.
C. Host-based firewall
D. DLP solution

Correct Answer: B
Section:
Explanation:
An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified.An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network12.
The other options are not the best ways to block unknown programs from executing:
Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object.An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing13.

Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system.A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing1.
DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data.A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing1.
Reference=1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting -- CompTIA Security+ SY0-701 -- 3.5, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

QUESTION 21
A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.
Which of the following teams will conduct this assessment activity?

A. White
B. Purple
C. Blue
D. Red

Correct Answer: D
Section:
Explanation:
A red team is a group of security professionals who perform offensive security assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4.Security Teams -- SY0-601 CompTIA Security+ : 1.8

QUESTION 22
A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

A. Serverless framework
B. Type 1 hvpervisor
C. SD-WAN
D. SDN

Correct Answer: A
Section:
Explanation:
A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.
A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.
SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.
SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.

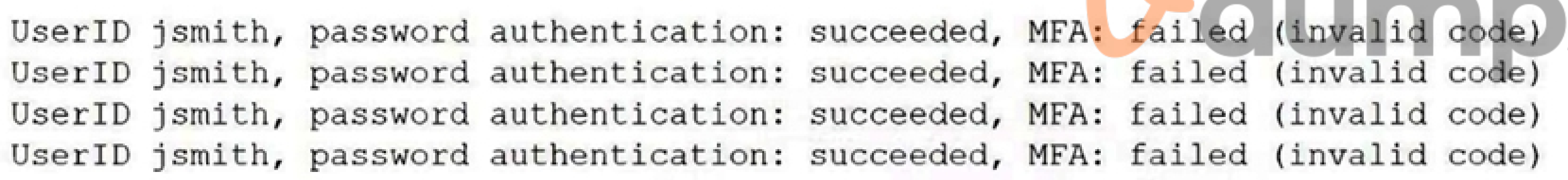
Reference=CompTIA Security+ SY0-701 Certification Study Guide, page 264-265;Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

QUESTION 23
A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

A. Tuning
B. Aggregating
C. Quarantining
D. Archiving

Correct Answer: A
Section:
Explanation:
Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope. Therefore, this is the best answer among the given options.Reference=Security Alerting and Monitoring Concepts and Tools -- CompTIA Security+ SY0-701: 4.3, video at 7:00;CompTIA Security+ SY0-701 Certification Study Guide, page 191.

QUESTION 24
A security analyst reviews domain activity logs and notices the following:



```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

A. The user jsmith's account has been locked out.
B. A keylogger is installed on [smith's workstation
C. An attacker is attempting to brute force ismith's account.
D. Ransomware has been deployed in the domain.

Correct Answer: C
Section:
Explanation:
Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2.Threat Actors and Attributes -- SY0-601 CompTIA Security+ : 1.1

QUESTION 25
A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

A. Clustering servers
B. Geographic dispersion
C. Load balancers
D. Off-site backups

Correct Answer: B
Section:
Explanation:
Geographic dispersion is a strategy that involves distributing the servers or data centers across different geographic locations. Geographic dispersion can help the company to mitigate the risk of weather events causing damage to the server room and downtime, as well as improve the availability, performance, and resilience of the network.Geographic dispersion can also enhance the disaster recovery and business continuity capabilities of the company, as it can provide backup and failover options in case of a regional outage or disruption12.
The other options are not the best ways to address the company's concern:
Clustering servers: This is a technique that involves grouping multiple servers together to act as a single system.Clustering servers can help to improve the performance, scalability, and fault tolerance of the network, but it does not protect the servers from physical damage or downtime caused by weather events, especially if the servers are located in the same room or building3.
Load balancers: These are devices or software that distribute the network traffic or workload among multiple servers or resources.Load balancers can help to optimize the utilization, efficiency, and reliability of the network, but they do not prevent the servers from being damaged or disrupted by weather events, especially if the servers are located in the same room or building4.
Off-site backups: These are copies of data or files that are stored in a different location than the original source. Off-site backups can help to protect the data from being lost or corrupted by weather events, but they do not prevent the servers from being damaged or disrupted by weather events, nor do they ensure the availability or continuity of the network services.
Reference=1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability -- CompTIA Security+ SY0-701 -- 3.4, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 984: CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

QUESTION 26
Which of the following is a primary security concern for a company setting up a BYOD program?

A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking

Correct Answer: D
Section:
Explanation:
Jailbreaking is a primary security concern for a company setting up a BYOD (Bring Your Own Device) program. Jailbreaking is the process of removing the manufacturer's or the carrier's restrictions on a device, such as a smartphone or a tablet, to gain root access and install unauthorized or custom software. Jailbreaking can compromise the security of the device and the data stored on it, as well as expose it to malware, viruses, or hacking. Jailbreaking can also violate the warranty and the terms of service of the device, and make it incompatible with the company's security policies and standards. Therefore, a company setting up a BYOD program should prohibit jailbreaking and enforce device compliance and encryption.Reference=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 76. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4, page 11.

QUESTION 27
An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a ''page not found'' error message. Which of the following types of social engineering attacks occurred?

A. Brand impersonation
B. Pretexting
C. Typosquatting
D. Phishing

Correct Answer: D

Section:
Explanation:
Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from a payment website that asked the employee to update contact information. The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one. The employee entered the log-in information, but received a ''page not found'' error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee's credentials for the payment website.Reference=Other Social Engineering Attacks -- CompTIA Security+ SY0-701 -- 2.2,CompTIA Security+: Social Engineering Techniques & Other Attack ... - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

QUESTION 28
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25 32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25 32 port 53 Access list outbound deny 0.0.0.0 0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 port 53
D. Access list outbound permit 10.50.10.25 32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0.0.0.0.0/0 port 53

Correct Answer: D
Section:
Explanation:
The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B).Reference= You can learn more about firewall ACLs and DNS in the following resources:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 4: Network Security1
Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 3.2: Firewall Rules2
TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 6: Network Security, Lecture 28: Firewall Rules3

QUESTION 29
A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A. SSO
B. LEAP
C. MFA
D. PEAP

Correct Answer: A
Section:
Explanation:
SSO stands forsingle sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems.SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials123.
B) LEAP stands forLightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks.LEAP is not related to SaaS applications or domain credentials4.
C) MFA stands formulti-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.
D) PEAP stands forProtected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.
Reference=1:Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications2: What is Single Sign-On (SSO)?- Definition from WhatIs.com3: Single sign-on - Wikipedia4: Lightweight Extensible Authentication

Protocol - Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

QUESTION 30

Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.

B. Employees who open an email attachment receive messages demanding payment in order to access files.

C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.

D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Correct Answer: A
Section:
Explanation:

A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data.The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to convince the victim to comply with the request12.

In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive's name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes.This is a common tactic used by BEC attackers to steal money from unsuspecting victims34.

Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key. Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority. Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company's email portal and capture their credentials.These are all types of cyberattacks, but they are not examples of BEC attacks.Reference=1: Business Email Compromise - CompTIA Security+ SY0-701 - 2.22: CompTIA Security+ SY0-701 Certification Study Guide3: Business Email Compromise: The 12 Billion Dollar Scam4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

QUESTION 31

A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?

A. Jump server

B. RADIUS

C. HSM

D. Load balancer

Correct Answer: A
Section:
Explanation:

A jump server is a device or virtual machine that acts as an intermediary between a user's workstation and a remote network segment. A jump server can be used to securely access servers or devices that are not directly reachable from the user's workstation, such as database servers. A jump server can also provide audit logs and access control for the remote connections.A jump server is also known as a jump box or a jump host12.

RADIUS is a protocol for authentication, authorization, and accounting of network access.RADIUS is not a device or a method to access remote servers, but rather a way to verify the identity and permissions of users or devices that request network access34.

HSM is an acronym for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. HSMs are used to protect sensitive data and applications, such as digital signatures, encryption, and authentication.HSMs are not used to access remote servers, but rather to enhance the security of the data and applications that reside on them5.

A load balancer is a device or software that distributes network traffic across multiple servers or devices, based on criteria such as availability, performance, or capacity. A load balancer can improve the scalability, reliability, and efficiency of network services, such as web servers, application servers, or database servers. A load balancer is not used to access remote servers, but rather to optimize the delivery of the services that run on them
.Reference=
How to access a remote server using a jump host
Jump server
RADIUS
Remote Authentication Dial-In User Service (RADIUS)

Hardware Security Module (HSM)
[What is an HSM?]
[Load balancing (computing)]
[What is Load Balancing?]

QUESTION 32
An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops
B. Containers
C. Thin clients
D. Workstations

Correct Answer: C
Section:
Explanation:
Thin clients are devices that rely on a server or a cloud service to perform most of the processing and storage tasks, while only providing a minimal interface for the user. Thin clients are low-cost solutions that can enable users on the shop floor to log in to the VDI (virtual desktop infrastructure) environment directly, without requiring a full-fledged computer or laptop.

QUESTION 33
Which of the following is an administrative control that would be most effective to reduce the occurrence of malware execution?

A. Security awareness training
B. Frequency of NIDS updates
C. Change control procedures
D. EDR reporting cycle

Correct Answer: A
Section:
Explanation:
Security awareness training is an administrative control that educates users on the best practices and policies for protecting the organization's data and systems from various threats, such as malware, phishing, social engineering, etc. Security awareness training can reduce the occurrence of malware execution by increasing the users' ability to recognize and avoid malicious links, attachments, downloads, or websites.

QUESTION 34
A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

A. MOA
B. SOW
C. MOU
D. SLA

Correct Answer: D
Section:
Explanation:
A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of

service levels and performance metrics that an SLA does.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

QUESTION 35
A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading

Correct Answer: C
Section:
Explanation:
Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty.Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 5072

QUESTION 36
An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

A. NGFW
B. WAF
C. TLS
D. SD-WAN

Correct Answer: B
Section:
Explanation:
A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data.Reference=Buffer Overflows -- CompTIA Security+ SY0-701 -- 2.3,Web Application Firewalls -- CompTIA Security+ SY0-701 -- 2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

QUESTION 37
An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multifactor authentication
B. Permissions assignment
C. Access management
D. Password complexity

Correct Answer: A

Section:
Explanation:
The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user's password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication. Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password.Reference= You can learn more about multifactor authentication and other security concepts in the following resources:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1
Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2
Multi-factor Authentication -- SY0-601 CompTIA Security+ : 2.43
TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication4
CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

QUESTION 38
An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

A. Typosquatting
B. Phishing
C. Impersonation
D. Vishing
E. Smishing
F. Misinformation

Correct Answer: B, E
Section:
Explanation:
Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware.Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action12. In this scenario, the text message that claims to be from the payroll department is an example of smishing.
Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target.Impersonation can be done through various channels, such as phone calls, emails, text messages, or in-person visits, and can be used to obtain information, access, or money from the victim34. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.
A) Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions.Typosquatting aims to exploit the common mistakes that users make when typing web addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads56. Typosquatting is not related to text messages or credential verification.
B) Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware.Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action78. Phishing is not related to text messages or credential verification.
D) Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit card numbers, or bank account details.Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply9. Vishing is not related to text messages or credential verification.
Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda . Misinformation is not related to text messages or credential verification. Reference=1:What is Smishing? | Definition and Examples | Kaspersky2: Smishing - Wikipedia3: Impersonation Attacks: What Are They and How Do You Protect Against Them?4: Impersonation - Wikipedia5:What is Typosquatting? | Definition and Examples | Kaspersky6: Typosquatting - Wikipedia7:What is Phishing? | Definition and Examples | Kaspersky8: Phishing - Wikipedia9:What is Vishing? | Definition and Examples | Kaspersky: Vishing - Wikipedia :What is Misinformation? | Definition and Examples | Britannica: Misinformation - Wikipedia

QUESTION 39

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:
''I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address.''
Which of the following are the best responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.
B. Add a smishing exercise to the annual company training.
C. Issue a general email warning to the company.
D. Have the CEO change phone numbers.
E. Conduct a forensic investigation on the CEO's phone.
F. Implement mobile device management.

Correct Answer: B, C
Section:
Explanation:
This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money.Reference=What Is Phishing | Cybersecurity | CompTIA,Phishing -- SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

QUESTION 40
A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain
B. A legally enforceable corporate acquisition policy
C. A right to audit clause in vendor contracts and SOWs
D. An in-depth penetration test of all suppliers and vendors

Correct Answer: A
Section:
Explanation:
Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM).It can pose serious risks to network quality, performance, safety, and reliability12.Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it3. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products. A thorough analysis of the supply chain can include the following steps:
Establishing a trusted relationship with the OEM and authorized resellers
Requesting documentation and certification of the hardware from the OEM or authorized resellers
Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components
Testing the hardware for functionality, performance, and security
Implementing a tracking system to monitor the hardware throughout its lifecycle
Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agenciesReference=1:Identify Counterfeit and Pirated Products - Cisco,2:What Is Hardware Security? Definition, Threats, and Best Practices,3:Beware of Counterfeit Network Equipment - TechNewsWorld, : Counterfeit Hardware: The Threat and How to Avoid It

QUESTION 41
Which of the following provides the details about the terms of a test with a third-party penetration tester?

A. Rules of engagement
B. Supply chain analysis
C. Right to audit clause

D. Due diligence

Correct Answer: A
Section:
Explanation:
Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:
The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.
The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.
The testing team credentials and the authorized tools and techniques that they can use.
The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.
The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.
The timeline and duration of the test, and the hours of operation and testing windows.
The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.
Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.
Reference= https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of-engagement/
https://bing.com/search?q=rules+of+engagement+penetration+testing

QUESTION 42
A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

A. Active
B. Passive
C. Defensive
D. Offensive

Correct Answer: A
Section:
Explanation:
Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information.
Reference=CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools.CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47.CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

QUESTION 43
Which of the following is required for an organization to properly manage its restore process in the event of system failure?

A. IRP
B. DRP
C. RPO
D. SDLC

Correct Answer: B
Section:
Explanation:

A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:
A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.
A business impact analysis that prioritizes the recovery of the most essential functions and data.
A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.
A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss.Reference=CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

QUESTION 44
An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

A. RDP server
B. Jump server
C. Proxy server
D. Hypervisor

Correct Answer: B
Section:
Explanation:
= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box.Reference=CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts.CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101.Other Network Appliances -- SY0-601 CompTIA Security+ : 3.3, Video 3:03.CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

QUESTION 45
A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

A. encryption=off\
B. http://
C. www.*.com
D. :443

Correct Answer: B
Section:
Explanation:
A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words ''gambling'', ''porn'', or ''malware'' in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components:protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.
To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.
The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic.Reference=CompTIA Security+

Study Guide (SY0-701), Chapter 2: Securing Networks, page 69.Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

QUESTION 46

During a security incident, the security operations team identified sustained network traffic from a malicious IP address:
10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32

B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0

C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0

D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

Correct Answer: B
Section:
Explanation:

A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.
Reference=Firewall Rules -- CompTIA Security+ SY0-401: 1.2,Firewalls -- SY0-601 CompTIA Security+ : 3.3,Firewalls -- CompTIA Security+ SY0-501,Understanding Firewall Rules -- CompTIA Network+ N10-005: 5.5,Configuring Windows Firewall -- CompTIA A+ 220-1102 -- 1.6.

QUESTION 47

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

A. Implementing a bastion host

B. Deploying a perimeter network

C. Installing a WAF

D. Utilizing single sign-on

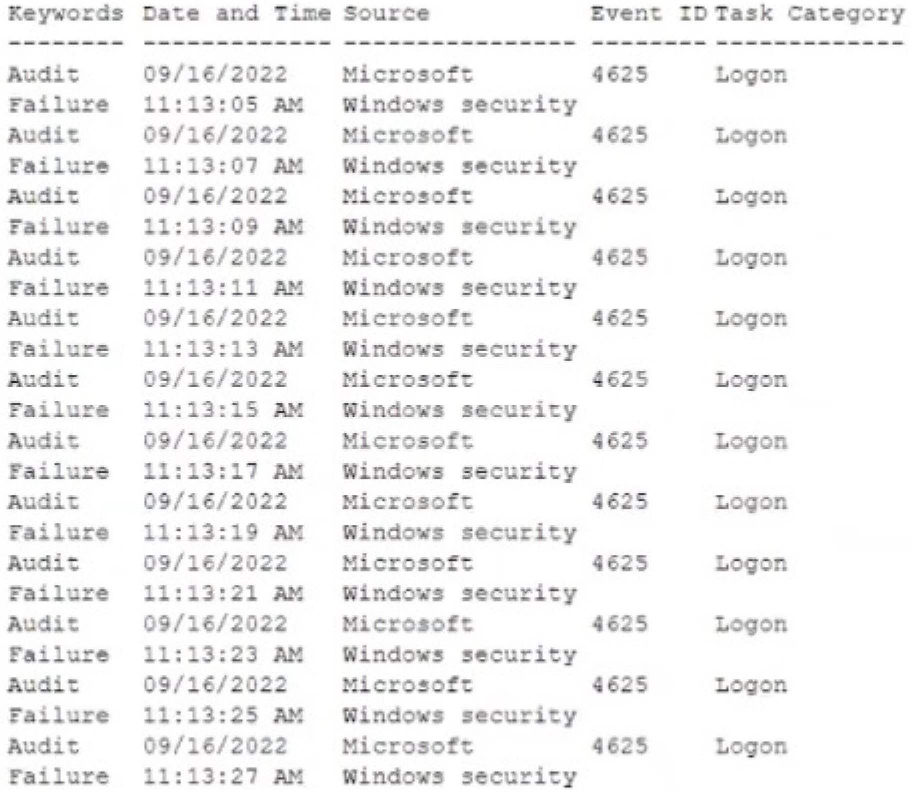
Correct Answer: A
Section:
Explanation:

A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic.A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes12.
A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense.A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise3.
Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access.A perimeter network can also increase the complexity and cost of network management and security4.
Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities.A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats5.

Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use.Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached6.Reference=1:Bastion host - Wikipedia,2:14 Best Practices to Secure SSH Bastion Host - goteleport.com,3:The Importance Of Bastion Hosts In Network Security,4:What is the network perimeter? | Cloudflare,5:What is a WAF? | Web Application Firewall explained,6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

QUESTION 48

An administrator is reviewing a single server's security logs and discovers the following;



```
Keywords Date and Time Source           Event  ID Task Category
-------- ------------- ---------------- -------- -------------
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:05 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:07 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:09 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:11 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:13 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:15 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:17 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:19 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:21 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:23 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:25 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:27 AM   Windows security
```

Which of the following best describes the action captured in this log file?

A. Brute-force attack
B. Privilege escalation
C. Failed password audit
D. Forgotten password by the user

Correct Answer: A
Section:
Explanation:
A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong.These are indicators of compromise (IoC) that suggest a brute-force attack is taking place.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 2231

QUESTION 49

A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Select two).

A. Key escrow
B. TPM presence

C. Digital signatures
D. Data tokenization
E. Public key management
F. Certificate authority linking

Correct Answer: A, B
Section:
Explanation:
Key escrowis a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.
TPM presenceis a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and performance of encryption by generating and protecting the keys within the chip, rather than relying on software or external devices. TPM presence also enables features such as secure boot, remote attestation, and device authentication.

QUESTION 50
A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware, which laid dormant for multiple weeks, across the network. Which of the following would have mitigated the spread?

A. IPS
B. IDS
C. WAF
D. UAT

Correct Answer: A
Section:
Explanation:

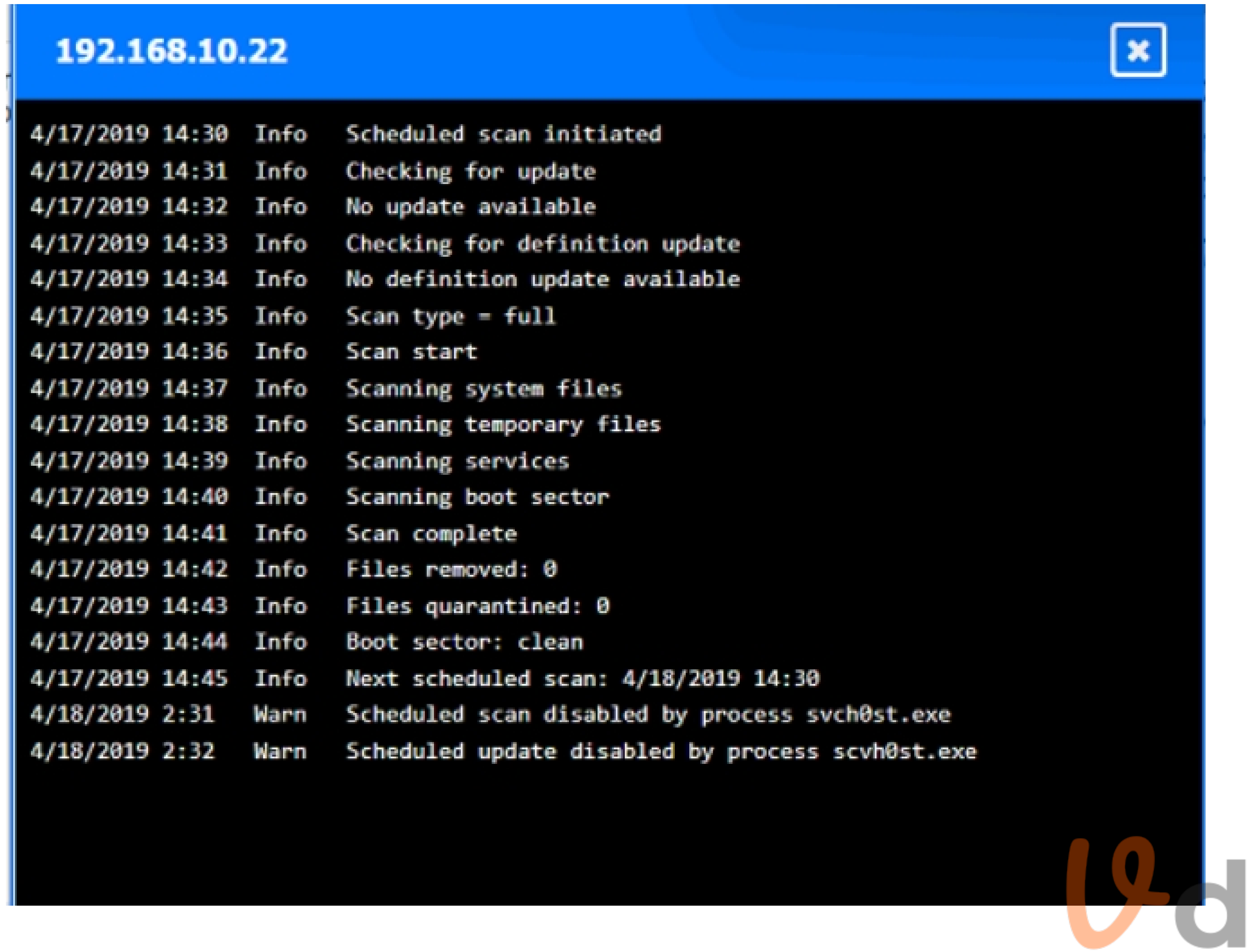
IPSstands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

QUESTION 51
A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

A. Attribute-based
B. Time of day
C. Role-based
D. Least privilege

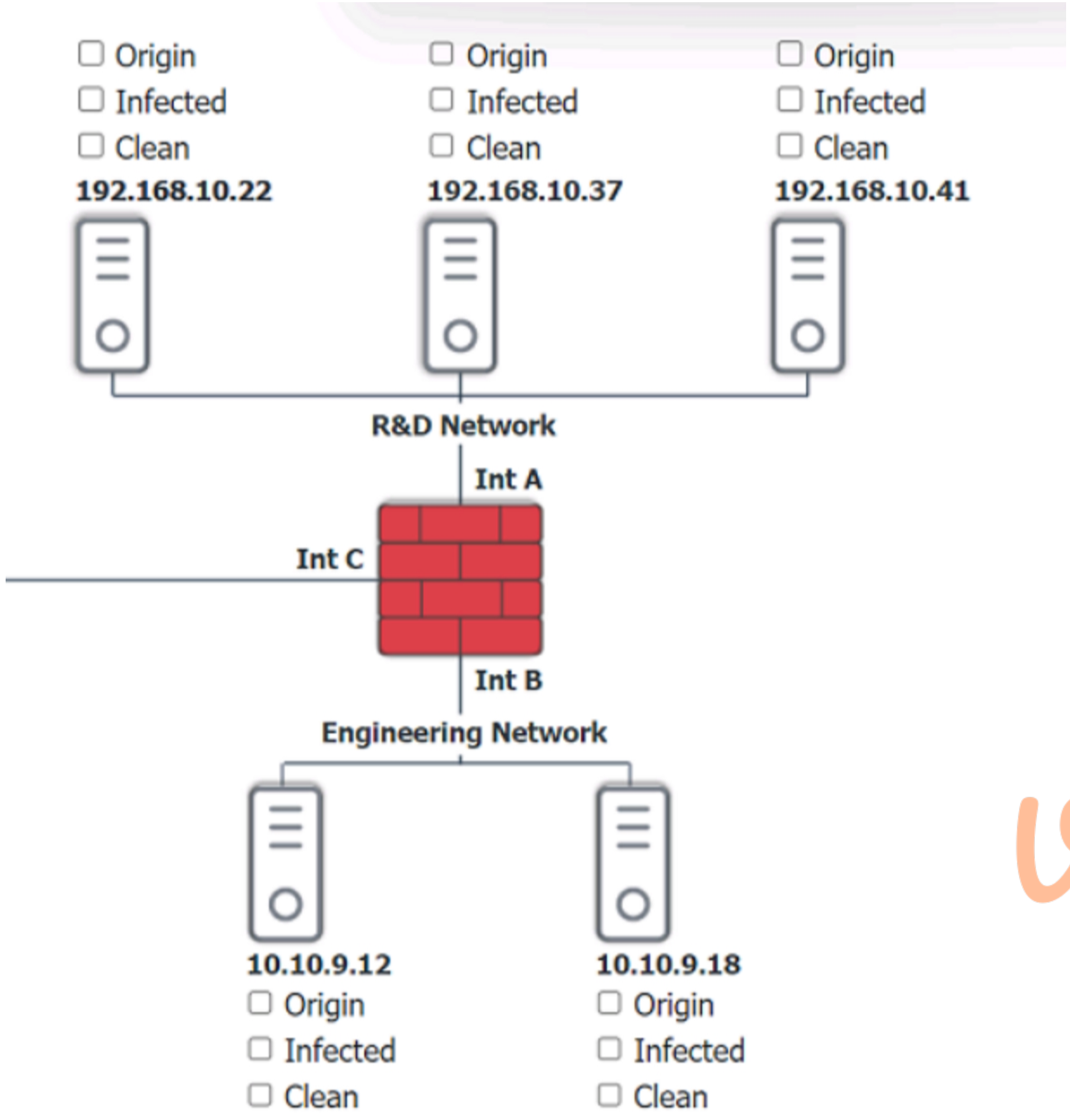
Correct Answer: D
Section:
Explanation:
The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer.Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

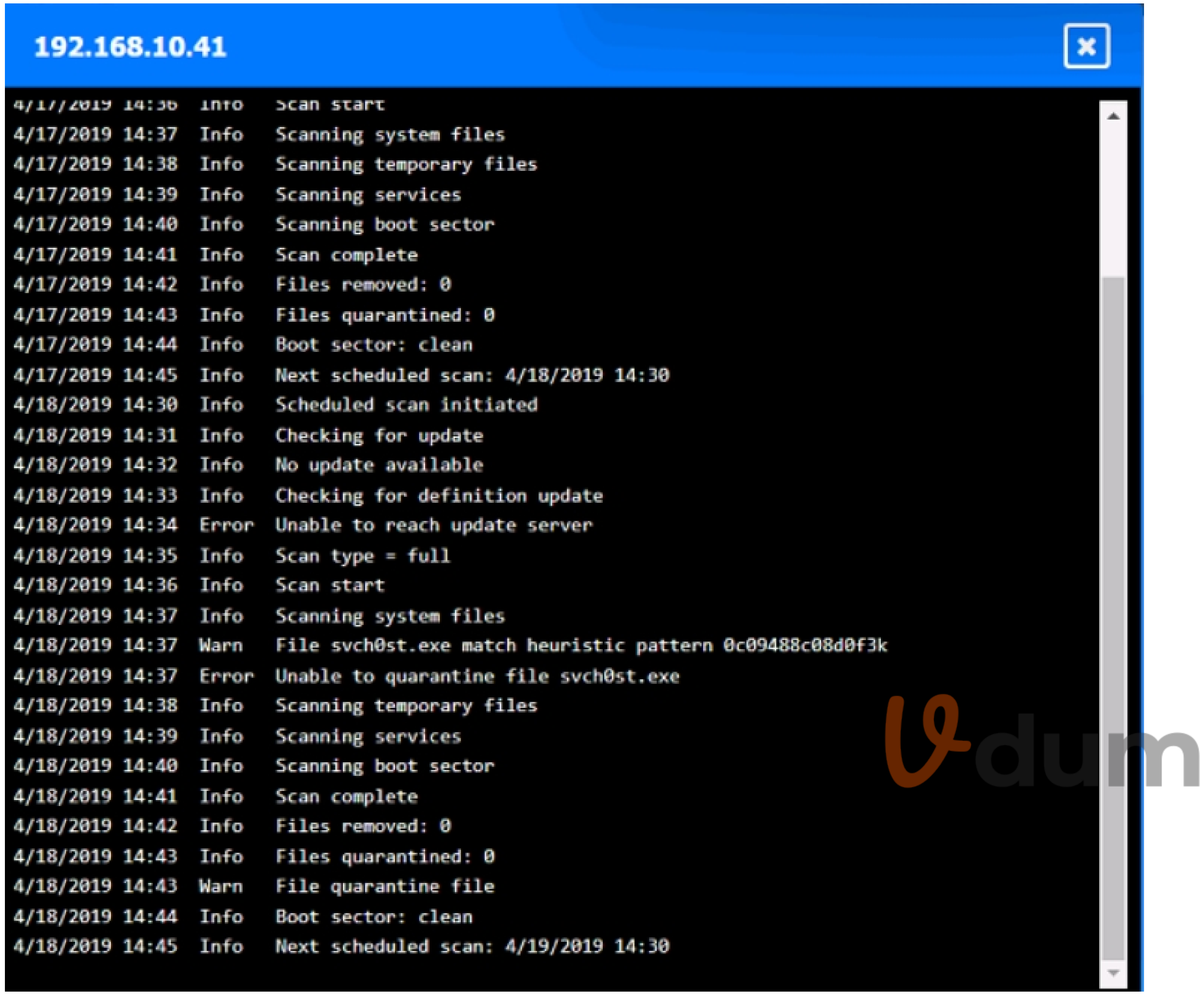
QUESTION 52
HOTSPOT
You are security administrator investigating a potential infection on a network.
Click on each host and firewall. Review all logs to determine which host originated the Infecton and then deny each remaining hosts clean or infected.



192.168.10.22

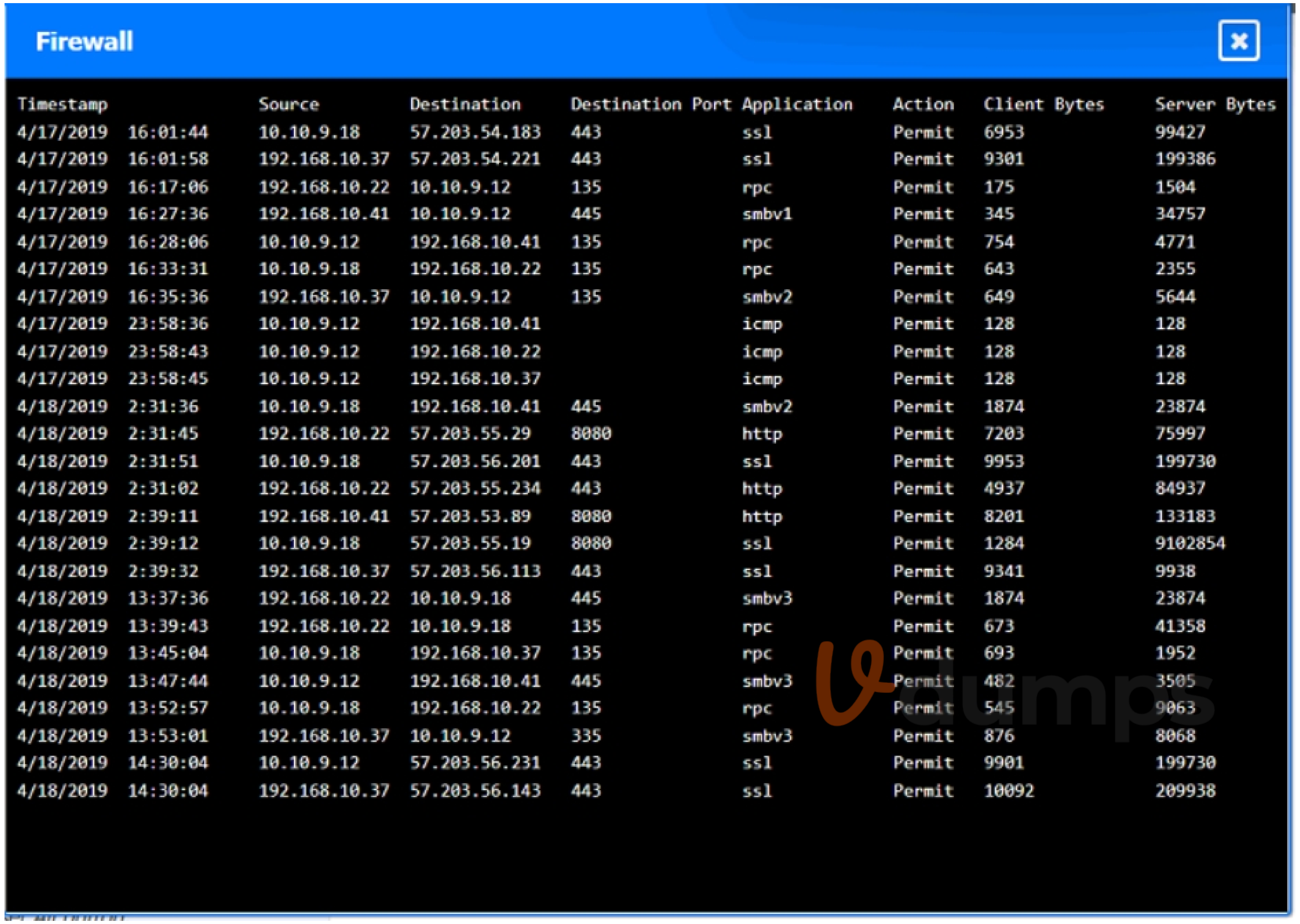
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31   Warn   Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32   Warn   Scheduled update disabled by process scvh0st.exe
```


□ Origin
□ Infected
□ Clean
192.168.10.22
□ Origin
□ Infected
□ Clean
192.168.10.37
□ Origin
□ Infected
□ Clean
192.168.10.41
R&D Network
Int A
Int C
Int B
Engineering Network
10.10.9.12
□ Origin
□ Infected
□ Clean
10.10.9.18
□ Origin
□ Infected
□ Clean

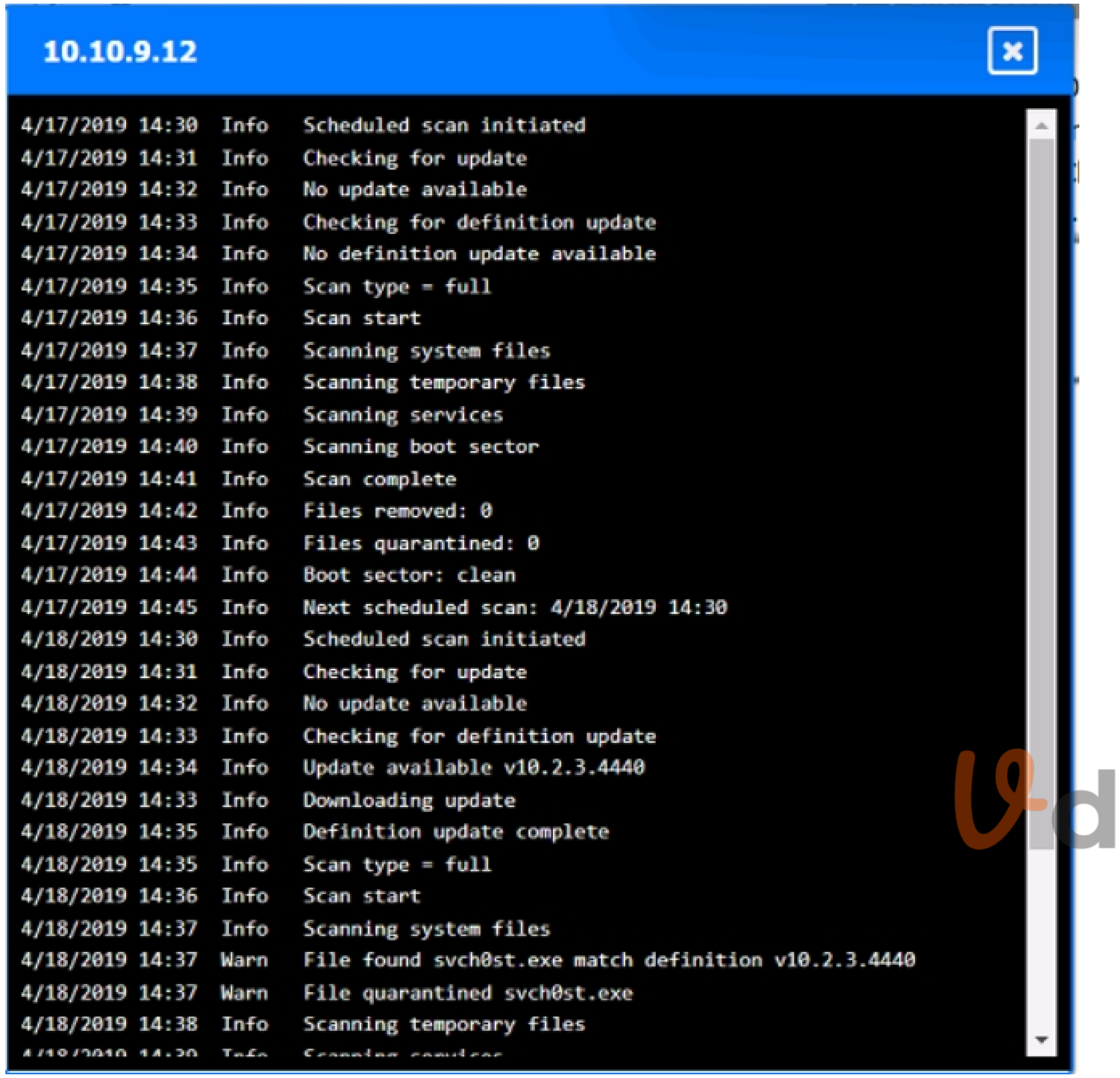


192.168.10.41

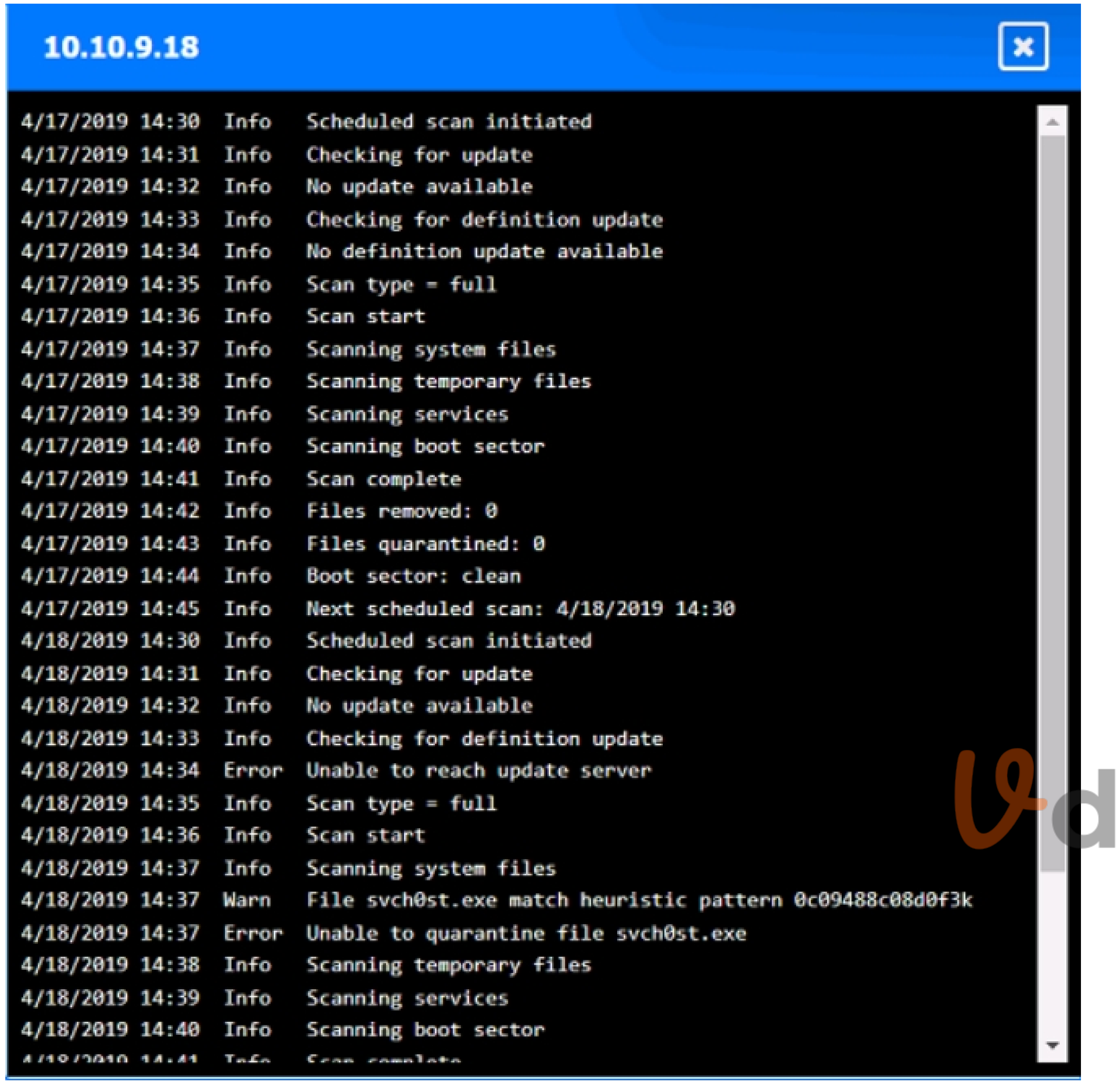
```
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```



```
Timestamp               Source         Destination     Destination Port Application    Action   Client Bytes     Server Bytes
4/17/2019  16:01:44     10.10.9.18     57.203.54.183   443              ssl            Permit   6953             99427
4/17/2019  16:01:58     192.168.10.37  57.203.54.221   443              ssl            Permit   9301             199386
4/17/2019  16:17:06     192.168.10.22  10.10.9.12      135              rpc            Permit   175              1504
4/17/2019  16:27:36     192.168.10.41  10.10.9.12      445              smbv1          Permit   345              34757
4/17/2019  16:28:06     10.10.9.12     192.168.10.41   135              rpc            Permit   754              4771
4/17/2019  16:33:31     10.10.9.18     192.168.10.22   135              rpc            Permit   643              2355
4/17/2019  16:35:36     192.168.10.37  10.10.9.12      135              smbv2          Permit   649              5644
4/17/2019  23:58:36     10.10.9.12     192.168.10.41                    icmp           Permit   128              128
4/17/2019  23:58:43     10.10.9.12     192.168.10.22                    icmp           Permit   128              128
4/17/2019  23:58:45     10.10.9.12     192.168.10.37                    icmp           Permit   128              128
4/18/2019  2:31:36      10.10.9.18     192.168.10.41   445              smbv2          Permit   1874             23874
4/18/2019  2:31:45      192.168.10.22  57.203.55.29    8080             http           Permit   7203             75997
4/18/2019  2:31:51      10.10.9.18     57.203.56.201   443              ssl            Permit   9953             199730
4/18/2019  2:31:02      192.168.10.22  57.203.55.234   443              http           Permit   4937             84937
4/18/2019  2:39:11      192.168.10.41  57.203.53.89    8080             http           Permit   8201             133183
4/18/2019  2:39:12      10.10.9.18     57.203.55.19    8080             ssl            Permit   1284             9102854
4/18/2019  2:39:32      192.168.10.37  57.203.56.113   443              ssl            Permit   9341             9938
4/18/2019  13:37:36     192.168.10.22  10.10.9.18      445              smbv3          Permit   1874             23874
4/18/2019  13:39:43     192.168.10.22  10.10.9.18      135              rpc            Permit   673              41358
4/18/2019  13:45:04     10.10.9.18     192.168.10.37   135              rpc            Permit   693              1952
4/18/2019  13:47:44     10.10.9.12     192.168.10.41   445              smbv3          Permit   482              3505
4/18/2019  13:52:57     10.10.9.18     192.168.10.22   135              rpc            Permit   545              9063
4/18/2019  13:53:01     192.168.10.37  10.10.9.12      335              smbv3          Permit   876              8068
4/18/2019  14:30:04     10.10.9.12     57.203.56.231   443              ssl            Permit   9901             199730
4/18/2019  14:30:04     192.168.10.37  57.203.56.143   443              ssl            Permit   10092            209938
```



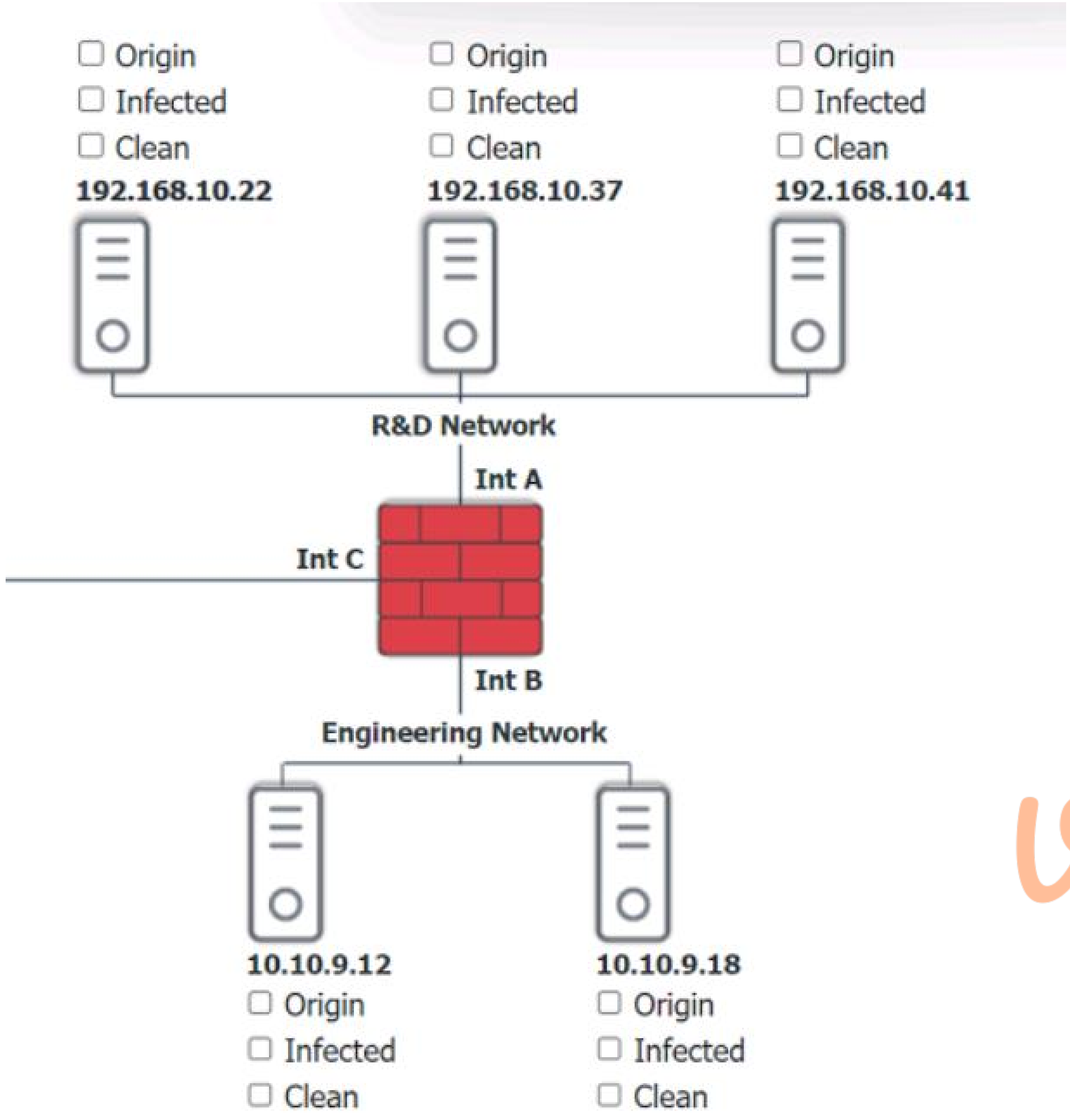
```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
```



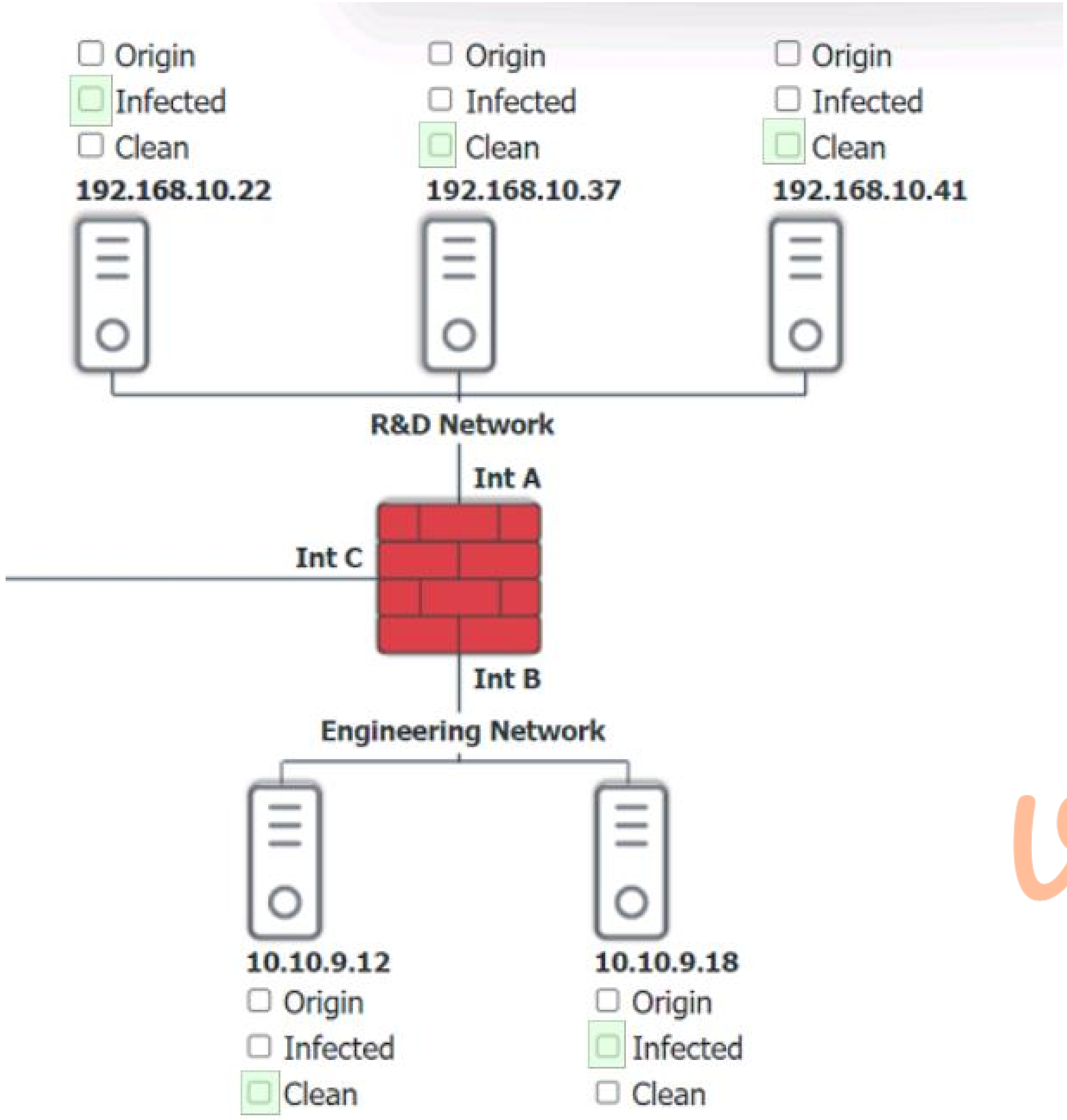
10.10.9.18

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
```

Hot Area:


□ Origin
□ Infected
□ Clean
192.168.10.22
□ Origin
□ Infected
□ Clean
192.168.10.37
□ Origin
□ Infected
□ Clean
192.168.10.41
R&D Network
Int A
Int C
Int B
Engineering Network
10.10.9.12
□ Origin
□ Infected
□ Clean
10.10.9.18
□ Origin
□ Infected
□ Clean

Answer Area:



Section:
Explanation:

QUESTION 53
Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition

Correct Answer: C
Section:
Explanation:
A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in

the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

QUESTION 54
Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation
B. Isolation
C. Hardening
D. Decommissioning

Correct Answer: B
Section:
Explanation:

QUESTION 55
Which of the following describes the process of concealing code or text inside a graphical image?

A. Symmetric encryption
B. Hashing
C. Data masking
D. Steganography

Correct Answer: D
Section:
Explanation:
Steganography is the process of hiding information within another medium, such as an image, audio, video, or text file. The hidden information is not visible or noticeable to the casual observer, and can only be extracted by using a specific technique or key.Steganography can be used for various purposes, such as concealing secret messages, watermarking, or evading detection by antivirus software12
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Cryptography and PKI, page 2332: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Cryptography and PKI, page 235

QUESTION 56
After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

A. Retain the emails between the security team and affected customers for 30 days.
B. Retain any communications related to the security breach until further notice.
C. Retain any communications between security members during the breach response.
D. Retain all emails from the company to affected customers for an indefinite period of time.

Correct Answer: B
Section:
Explanation:
A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party's case.A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena12
In this scenario, the company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to

the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance.The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss34
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 3032: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 3053: Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro54: The Legal Implications and Consequences of a Data Breach6

QUESTION 57
A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:
. Something you know
. Something you have
. Something you are
Which of the following would accomplish the manager's goal?

A. Domain name, PKI, GeolP lookup
B. VPN IP address, company ID, facial structure
C. Password, authentication token, thumbprint
D. Company URL, TLS certificate, home address

Correct Answer: C
Section:
Explanation:
The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager's goal of implementing multifactor authentication that uses something you know, something you have, and something you are.
Something you know is a type of authentication factor that relies on the user's knowledge of a secret or personal information, such as a password, a PIN, or a security question.A password is a common example of something you know that can be used to access a VPN12
Something you have is a type of authentication factor that relies on the user's possession of a physical object or device, such as a smart card, a token, or a smartphone.An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12
Something you are is a type of authentication factor that relies on the user's biometric characteristics, such as a fingerprint, a face, or an iris.A thumbprint is a common example of something you are that can be used to scan and verify the user's identity to access a VPN12
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Identity and Access Management, page 1772: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4: Identity and Access Management, page 179

QUESTION 58
A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

A. Set the maximum data retention policy.
B. Securely store the documents on an air-gapped network.
C. Review the documents' data classification policy.
D. Conduct a tabletop exercise with the team.

Correct Answer: D
Section:
Explanation:
A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents.

QUESTION 59
Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.
Which of the following changes would allow users to access the site?

A. Creating a firewall rule to allow HTTPS traffic
B. Configuring the IPS to allow shopping
C. Tuning the DLP rule that detects credit card data
D. Updating the categorization in the content filter

Correct Answer: D
Section:
Explanation:
A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow access to the website instead of blocking it.

QUESTION 60
An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user. Which of the following best describes the type of attack that occurred?

A. Insider threat
B. Social engineering
C. Watering-hole
D. Unauthorized attacker

Correct Answer: A
Section:
Explanation:

An insider threat is a type of attack that originates from someone who has legitimate access to an organization's network, systems, or data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, as they abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage.

QUESTION 61
Which of the following automation use cases would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company?

A. Provisioning resources
B. Disabling access
C. Reviewing change approvals
D. Escalating permission requests

Correct Answer: B
Section:
Explanation:
Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.

QUESTION 62
Which of the following must be considered when designing a high-availability network? (Select two).

A. Ease of recovery

B. Ability to patch
C. Physical isolation
D. Responsiveness
E. Attack surface
F. Extensible authentication

Correct Answer: A, E
Section:
Explanation:
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.
Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation.
Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security.

QUESTION 63
Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

A. Encryption
B. Hashing
C. Masking
D. Tokenization

Correct Answer: C
Section:
Explanation:
Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

QUESTION 64
An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

A. Virus
B. Trojan
C. Spyware
D. Ransomware

Correct Answer: D
Section:
Explanation:
Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files.The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms1.

QUESTION 65

A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.
Which of the following is the most important consideration during development?

A. Scalability
B. Availability
C. Cost
D. Ease of deployment

Correct Answer: B
Section:
Explanation:
Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users.The web application should be designed to handle high traffic, prevent denial-of-service attacks, and have backup and recovery plans in case of failures2.

QUESTION 66
Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).

A. Fencing
B. Video surveillance
C. Badge access
D. Access control vestibule
E. Sign-in sheet
F. Sensor

Correct Answer: C, D
Section:
Explanation:
Badge access and access control vestibule are two of the best ways to ensure only authorized personnel can access a secure facility. Badge access requires the personnel to present a valid and authenticated badge to a reader or scanner that grants or denies access based on predefined rules and permissions. Access control vestibule is a physical security measure that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure area. The personnel must enter the vestibule and wait for the first door to close and lock before the second door can be opened.This prevents tailgating or piggybacking by unauthorized individuals.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, pages 197-1981

QUESTION 67
A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

A. Processor
B. Custodian
C. Subject
D. Owner

Correct Answer: C
Section:
Explanation:
According to the CompTIA Security+ SY0-701 Certification Study Guide, data subjects are the individuals whose personal data is collected, processed, or stored by an organization. Data subjects have certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data. Data subjects are different from data owners, who are the individuals or entities that have the authority and

responsibility to determine how data is classified, protected, and used. Data subjects are also different from data processors, who are the individuals or entities that perform operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting data. Data subjects are also different from data custodians, who are the individuals or entities that implement the security controls and procedures specified by the data owner to protect data while in transit and at rest.
Reference CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Data Security, page 511

QUESTION 68
Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

A. Impersonation
B. Disinformation
C. Watering-hole
D. Smishing

Correct Answer: C
Section:
Explanation:
A watering-hole attack is a type of cyberattack that targets groups of users by infecting websites that they commonly visit. The attackers exploit vulnerabilities to deliver a malicious payload to the organization's network. The attack aims to infect users' computers and gain access to a connected corporate network. The attackers target websites known to be popular among members of a particular organization or demographic.The attack differs from phishing and spear-phishing attacks, which typically attempt to steal data or install malware onto users' devices1
In this scenario, the compromised industry blog is the watering hole that the attackers used to spread malware across the company's network. The attackers likely chose this blog because they knew that the employees of the company were interested in its content and visited it frequently. The attackers may have injected malicious code into the blog or redirected the visitors to a spoofed website that hosted the malware. The malware then infected the employees' computers and propagated to the network.
Reference 1:Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

QUESTION 69
A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

A. Insurance
B. Patching
C. Segmentation
D. Replacement

Correct Answer: C
Section:
Explanation:
Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

QUESTION 70
A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest
B. Masking
C. Data classification
D. Permission restrictions

Correct Answer: A
Section:
Explanation:
Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17-18, 372-373

QUESTION 71
Which of the following would be best suited for constantly changing environments?

A. RTOS
B. Containers
C. Embedded systems
D. SCADA

Correct Answer: B
Section:
Explanation:
Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update.Containers can also support microservices architectures, which enable faster and more frequent delivery of software features.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 5121

QUESTION 72
A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

A. Changing the remote desktop port to a non-standard number
B. Setting up a VPN and placing the jump server inside the firewall
C. Using a proxy for web connections from the remote desktop server
D. Connecting the remote server to the domain and increasing the password length

Correct Answer: B
Section:
Explanation:
A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network.This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-3831; Chapter 9: Network Security, page 441-4421

QUESTION 73
Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?

A. Remote access points should fail closed.
B. Logging controls should fail open.
C. Safety controls should fail open.
D. Logical security controls should fail closed.

Correct Answer: C
Section:
Explanation:
Safety controls are security controls that are designed to protect human life and physical assets from harm or damage. Examples of safety controls include fire alarms, sprinklers, emergency exits, backup generators, and surge protectors. Safety controls should fail open, which means that they should remain operational or allow access when a failure or error occurs. Failing open can prevent or minimize the impact of a disaster, such as a fire, flood, earthquake, or power outage, on human life and physical assets. For example, if a fire alarm fails, it should still trigger the sprinklers and unlock the emergency exits, rather than remain silent and locked. Failing open can also ensure that essential services, such as healthcare, transportation, or communication, are available during a crisis. Remote access points, logging controls, and logical security controls are other types of security controls, but they should not fail open in a data center. Remote access points are security controls that allow users or systems to access a network or a system from a remote location, such as a VPN, a web portal, or a wireless access point. Remote access points should fail closed, which means that they should deny access when a failure or error occurs. Failing closed can prevent unauthorized or malicious access to the data center's network or systems, such as by hackers, malware, or rogue devices. Logging controls are security controls that record and monitor the activities and events that occur on a network or a system, such as user actions, system errors, security incidents, or performance metrics. Logging controls should also fail closed, which means that they should stop or suspend the activities or events when a failure or error occurs. Failing closed can prevent data loss, corruption, or tampering, as well as ensure compliance with regulations and standards. Logical security controls are security controls that use software or code to protect data and systems from unauthorized or malicious access, modification, or destruction, such as encryption, authentication, authorization, or firewall. Logical security controls should also fail closed, which means that they should block or restrict access when a failure or error occurs. Failing closed can prevent data breaches, cyberattacks, or logical flaws, as well as ensure confidentiality, integrity, and availability of data and systems.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143, 372-373, 376-377

QUESTION 74
A systems administrator is working on a solution with the following requirements:
* Provide a secure zone.
* Enforce a company-wide access control policy.
* Reduce the scope of threats.
Which of the following is the systems administrator setting up?

A. Zero Trust
B. AAA
C. Non-repudiation
D. CIA

Correct Answer: A
Section:
Explanation:
Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.
5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.
8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

QUESTION 75
Which of the following describes the maximum allowance of accepted risk?

A. Risk indicator
B. Risk level
C. Risk score

D. Risk threshold

Correct Answer: D
Section:
Explanation:
Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 34;Accepting Risk: Definition, How It Works, and Alternatives

QUESTION 76
Which of the following incident response activities ensures evidence is properly handied?

A. E-discovery
B. Chain of custody
C. Legal hold
D. Preservation

Correct Answer: B
Section:
Explanation:
Chain of custody is the process of documenting and preserving the integrity of evidence collected during an incident response. It involves recording the details of each person who handled the evidence, the time and date of each transfer, and the location where the evidence was stored. Chain of custody ensures that the evidence is admissible in legal proceedings and can be traced back to its source. E-discovery, legal hold, and preservation are related concepts, but they do not ensure evidence is properly handled.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487;NIST SP 800-61: 3.2. Evidence Gathering and Handling

QUESTION 77
Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

A. Mitigate
B. Accept
C. Transfer
D. Avoid

Correct Answer: A
Section:
Explanation:
Mitigate is the risk management strategy that involves reducing the likelihood or impact of a risk. If a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the enterprise should adopt the mitigate strategy first to address the existing vulnerabilities and gaps in the application. This could involve applying patches, updates, or configuration changes to the application, or adding additional layers of security controls around the application. Accept, transfer, and avoid are other risk management strategies, but they are not the best options for this scenario. Accept means acknowledging the risk and accepting the consequences without taking any action. Transfer means shifting the risk to a third party, such as an insurance company or a vendor. Avoid means eliminating the risk by removing the source or changing the process.These strategies may not be feasible or desirable for a legacy application that is critical to business operations and has no preventative controls in place.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; A Risk-Based Framework for Legacy System Migration and Deprecation2

QUESTION 78
Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

A. Red
B. Blue
C. Purple

D. Yellow

Correct Answer: C
Section:
Explanation:
Purple is the team that combines both offensive and defensive testing techniques to protect an organization's critical systems. Purple is not a separate team, but rather a collaboration between the red team and the blue team. The red team is the offensive team that simulates attacks and exploits vulnerabilities in the organization's systems. The blue team is the defensive team that monitors and protects the organization's systems from real and simulated threats. The purple team exists to ensure and maximize the effectiveness of the red and blue teams by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that improves the overall security posture of the organization. Red, blue, and yellow are other types of teams involved in security testing, but they do not combine both offensive and defensive techniques.The yellow team is the team that builds software solutions, scripts, and other programs that the blue team uses in the security testing.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams3

QUESTION 79
A company is working with a vendor to perform a penetration test Which of the following includes an estimate about the number of hours required to complete the engagement?

A. SOW
B. BPA
C. SLA
D. NDA

Correct Answer: A
Section:
Explanation:
A statement of work (SOW) is a document that defines the scope, objectives, deliverables, timeline, and costs of a project or service. It typically includes an estimate of the number of hours required to complete the engagement, as well as the roles and responsibilities of the parties involved. A SOW is often used for penetration testing projects to ensure that both the client and the vendor have a clear and mutual understanding of what is expected and how the work will be performed. A business partnership agreement (BPA), a service level agreement (SLA), and a non-disclosure agreement (NDA) are different types of contracts that may be related to a penetration testing project, but they do not include an estimate of the number of hours required to complete the engagement.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 492;What to Look For in a Penetration Testing Statement of Work?

QUESTION 80
The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening'?

A. Using least privilege
B. Changing the default password
C. Assigning individual user IDs
D. Reviewing logs more frequently

Correct Answer: B
Section:
Explanation:
Changing the default password for the local administrator account on a VPN appliance is a basic security measure that would have most likely prevented the unexpected login to the remote management interface. Default passwords are often easy to guess or publicly available, and attackers can use them to gain unauthorized access to devices and systems. Changing the default password to a strong and unique one reduces the risk of brute-force attacks and credential theft. Using least privilege, assigning individual user IDs, and reviewing logs more frequently are also good security practices, but they are not as effective as changing the default password in preventing the unexpected login.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 116;Local Admin Accounts - Security Risks and Best Practices (Part 1)

QUESTION 81
Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

A. Software as a service
B. Infrastructure as code
C. Internet of Things
D. Software-defined networking

Correct Answer: B
Section:
Explanation:
Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

QUESTION 82
An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

A. ACL
B. DLP
C. IDS
D. IPS

Correct Answer: D
Section:
Explanation:

An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

QUESTION 83
During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

Correct Answer: A, C
Section:
Explanation:
Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness.Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess.Reference:CompTIA Security+

Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-3131

QUESTION 84
A company is implementing a vendor's security tool in the cloud. The security director does not want to manage users and passwords specific to this tool but would rather utilize the company's standard user directory. Which of the following should the company implement?

A. 802.1X
B. SAML
C. RADIUS
D. CHAP

Correct Answer: B
Section:
Explanation:
The company should implement Security Assertion Markup Language (SAML) to integrate the vendor's security tool with their existing user directory. SAML is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP), enabling Single Sign-On (SSO). This allows the company to use its existing directory services for authentication, avoiding the need to manage a separate set of user credentials for the new tool.
CompTIA Security+ SY0-701 Course Content: Domain 4: Identity and Access Management, which includes SAML as a key identity federation standard for SSO.
CompTIA Security+ Study Guide (SY0-601): Chapter 8, 'Identity and Access Management,' details the role of SAML in enabling SSO by utilizing an existing identity provider.

QUESTION 85
An employee fell for a phishing scam, which allowed an attacker to gain access to a company PC. The attacker scraped the PC's memory to find other credentials. Without cracking these credentials, the attacker used them to move laterally through the corporate network. Which of the following describes this type of attack?

A. Privilege escalation
B. Buffer overflow
C. SQL injection
D. Pass-the-hash

Correct Answer: D
Section:
Explanation:
The scenario describes an attacker who obtained credentials from a compromised system's memory and used them without cracking to move laterally within the network. This technique is known as a 'pass-the-hash' attack, where the attacker captures hashed credentials (e.g., NTLM hashes) and uses them to authenticate and gain access to other systems without needing to know the plaintext password. This is a common attack method in environments where weak security practices or outdated protocols are in use.
Reference =
CompTIA Security+ SY0-701 Course Content: The course discusses credential-based attacks like pass-the-hash, emphasizing their impact and the importance of protecting credential stores.

QUESTION 86
A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

A. Serverless architecture
B. Thin clients
C. Private cloud
D. Virtual machines

Correct Answer: A
Section:

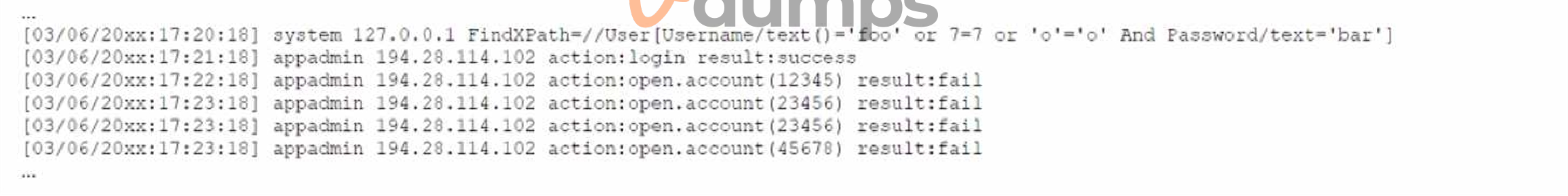
Explanation:
Serverless architecture allows companies to deploy code without managing the underlying infrastructure. This approach significantly reduces the time and expense involved in code deployment because developers can focus solely on writing code, while the cloud provider manages the servers, scaling, and maintenance. Serverless computing also enables automatic scaling and pay-per-execution billing, which further optimizes costs.
Reference =
CompTIA Security+ SY0-701 Course Content: The course covers cloud technologies, including serverless architectures, which are highlighted as a method to streamline and reduce costs associated with code deployment.

QUESTION 87
A company currently uses passwords for logging in to company-owned devices and wants to add a second authentication factor Per corporate policy, users are not allowed to have smartphones at their desks Which of the following would meet these requirements?

A. Smart card
B. PIN code
C. Knowledge-based question
D. Secret key

Correct Answer: A
Section:
Explanation:
A smart card is a physical device that contains an embedded integrated circuit chip that can store and process data. A smart card can be used as a second authentication factor, in addition to a password, to verify the identity of a user who wants to log in to company-owned devices. A smart card requires a smart card reader to access the data on the chip, which adds an extra layer of security. A smart card meets the requirements of the company because it does not involve a smartphone or any other device that is not allowed at the desks

QUESTION 88
A security analyst receives a SIEM alert that someone logged in to the app admin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:



```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
...
```

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Correct Answer: A
Section:
Explanation:
A replay attack is a type of network attack where an attacker captures and retransmits a valid data transmission, such as a login request, to gain unauthorized access or impersonate a legitimate user.
In this case, the attacker may have captured the credentials of the app admin test account and used them to log in to the application. The application log shows multiple failed login attempts from different IP addresses, which indicates a replay attack.

QUESTION 89

An organization is having difficulty correlating events from its individual AV. EDR. DLP. SWG. WAF, MDM. HIPS, and CASB systems. Which of the following is the best way to improve the situation?

A. Remove expensive systems that generate few alerts.
B. Modify the systems to alert only on critical issues.
C. Utilize a SIEM to centralize logs and dashboards.
D. Implement a new syslog/NetFlow appliance.

Correct Answer: C
Section:
Explanation:
A SIEM (Security Information and Event Management) is a system that collects, analyzes, and correlates data from multiple sources, such as AV (antivirus), EDR (endpoint detection and response), DLP (data loss prevention), SWG (secure web gateway), WAF (web application firewall), MDM (mobile device management), HIPS (host intrusion prevention system), and CASB (cloud access security broker). A SIEM can help improve the situation by providing a centralized view of the security posture, alerts, and incidents across the organization.

QUESTION 90
An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A. Smishing
B. Disinformation
C. Impersonating
D. Whaling

Correct Answer: D
Section:
Explanation:
Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link.Whaling is also called CEO fraud or business email compromise2.

QUESTION 91
An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

A. Secured zones
B. Subject role
C. Adaptive identity
D. Threat scope reduction

Correct Answer: A
Section:
Explanation:
Secured zones are a key component of the Zero Trust data plane, which is the layer where data is stored, processed, and transmitted. Secured zones are logical or physical segments of the network that isolate data and resources based on their sensitivity and risk.Secured zones enforce granular policies and controls to prevent unauthorized access and lateral movement within the network1.

QUESTION 92
An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

A. Data in use
B. Data in transit

C. Geographic restrictions
D. Data sovereignty

Correct Answer: B
Section:
Explanation:
Data in transit is data that is moving from one location to another, such as over a network or through the air. Data in transit is vulnerable to interception, modification, or theft by malicious actors.A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it2.

QUESTION 93
The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT
B. Insider threat
C. Data exfiltration
D. Service disruption

Correct Answer: A
Section:
Explanation:
Shadow IT is the term used to describe the use of unauthorized or unapproved IT resources within an organization. The marketing department set up its own project management software without telling the appropriate departments, such as IT, security, or compliance.This could pose a risk to the organization's security posture, data integrity, and regulatory compliance1.

QUESTION 94
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Correct Answer: D
Section:
Explanation:
A firewall ACL (access control list) is a set of rules that determines which traffic is allowed or denied by the firewall. The rules are processed in order, from top to bottom, until a match is found. The syntax of a firewall ACL rule is:
Access list <direction> <source address> <destination address>
To limit outbound DNS traffic originating from the internal network, the firewall ACL should allow only the device with the IP address 10.50.10.25 to send DNS requests to any destination on port 53, and deny all other outbound traffic on port 53. The correct firewall ACL is:
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
The first rule permits outbound traffic from the source address 10.50.10.25/32 (a single host) to any destination address (0.0.0.0/0) on port 53 (DNS).The second rule denies all other outbound traffic on port 532.

QUESTION 95
A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems. Which of the following strategies should the company use to achieve this security requirement?

A. Microservices

B. Containerization
C. Virtualization
D. Infrastructure as code

Correct Answer: C
Section:
Explanation:

QUESTION 96
An organization wants to ensure the integrity of compiled binaries in the production environment. Which of the following security measures would best support this objective?

A. Input validation
B. Code signing
C. SQL injection
D. Static analysis

Correct Answer: B
Section:
Explanation:
To ensure the integrity of compiled binaries in the production environment, the best security measure is code signing. Code signing uses digital signatures to verify the authenticity and integrity of the software, ensuring that the code has not been tampered with or altered after it was signed.
Code signing: Involves signing code with a digital signature to verify its authenticity and integrity, ensuring the compiled binaries have not been altered.
Input validation: Ensures that only properly formatted data enters an application but does not verify the integrity of compiled binaries.
SQL injection: A type of attack, not a security measure.
Static analysis: Analyzes code for vulnerabilities and errors but does not ensure the integrity of compiled binaries in production.

QUESTION 97
A systems administrator would like to deploy a change to a production system. Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

A. Backout plan
B. Impact analysis
C. Test procedure
D. Approval procedure

Correct Answer: A
Section:
Explanation:
To demonstrate that the system can be restored to a working state in the event of a performance issue after deploying a change, the systems administrator must submit a backout plan. A backout plan outlines the steps to revert the system to its previous state if the new deployment causes problems.
Backout plan: Provides detailed steps to revert changes and restore the system to its previous state in case of issues, ensuring minimal disruption and quick recovery.
Impact analysis: Evaluates the potential effects of a change but does not provide steps to revert changes.
Test procedure: Details the steps for testing the change but does not address restoring the system to a previous state.
Approval procedure: Involves obtaining permissions for the change but does not ensure system recovery in case of issues.

QUESTION 98
A security administrator is configuring fileshares. The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties. Which of the

following best describes why the administrator performed these actions?

A. Encryption standard compliance
B. Data replication requirements
C. Least privilege
D. Access control monitoring

Correct Answer: C
Section:
Explanation:
The security administrator's actions of removing default permissions and adding permissions only for users who need access as part of their job duties best describe the principle of least privilege. This principle ensures that users are granted the minimum necessary access to perform their job functions, reducing the risk of unauthorized access or data breaches.
Least privilege: Limits access rights for users to the bare minimum necessary for their job duties, enhancing security by reducing potential attack surfaces.
Encryption standard compliance: Involves meeting encryption requirements, but it does not explain the removal and assignment of specific permissions.
Data replication requirements: Focus on duplicating data across different systems for redundancy and availability, not related to user permissions.
Access control monitoring: Involves tracking and reviewing access to resources, but the scenario is about setting permissions, not monitoring them.

QUESTION 99
Which of the following describes effective change management procedures?

A. Approving the change after a successful deployment
B. Having a backout plan when a patch fails
C. Using a spreadsheet for tracking changes
D. Using an automatic change control bypass for security updates

Correct Answer: B
Section:
Explanation:
Effective change management procedures include having a backout plan when a patch fails. A backout plan ensures that there are predefined steps to revert the system to its previous state if the new change or patch causes issues, thereby minimizing downtime and mitigating potential negative impacts.
Having a backout plan when a patch fails: Essential for ensuring that changes can be safely reverted in case of problems, maintaining system stability and availability.
Approving the change after a successful deployment: Changes should be approved before deployment, not after.
Using a spreadsheet for tracking changes: While useful for documentation, it is not a comprehensive change management procedure.
Using an automatic change control bypass for security updates: Bypassing change control can lead to unapproved and potentially disruptive changes.

QUESTION 100
Which of the following tasks is typically included in the BIA process?

A. Estimating the recovery time of systems
B. Identifying the communication strategy
C. Evaluating the risk management plan
D. Establishing the backup and recovery procedures
E. Developing the incident response plan

Correct Answer: A
Section:
Explanation:
Estimating the recovery time of systems is a task typically included in the Business Impact Analysis (BIA) process. BIA involves identifying the critical functions of a business and determining the impact of a disruption. This

includes estimating how long it will take to recover systems and resume normal operations.
Estimating the recovery time of systems: A key component of BIA, which helps in understanding the time needed to restore systems and services after a disruption.
Identifying the communication strategy: Typically part of the incident response plan, not BIA.
Evaluating the risk management plan: Part of risk management, not specifically BIA.
Establishing the backup and recovery procedures: Important for disaster recovery, not directly part of BIA.
Developing the incident response plan: Focuses on responding to security incidents, not on the impact analysis.

QUESTION 101
An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Select two).

A. Disable default accounts.
B. Add the server to the asset inventory.
C. Remove unnecessary services.
D. Document default passwords.
E. Send server logs to the SIEM.
F. Join the server to the corporate domain.

Correct Answer: A, C
Section:
Explanation:
To perform server hardening before deployment, the administrator should disable default accounts and remove unnecessary services. These steps are crucial to reducing the attack surface and enhancing the security of the server.
Disable default accounts: Default accounts often come with default credentials that are well-known and can be exploited by attackers. Disabling these accounts helps prevent unauthorized access.
Remove unnecessary services: Unnecessary services can introduce vulnerabilities and be exploited by attackers. Removing them reduces the number of potential attack vectors.
Add the server to the asset inventory: Important for tracking and management but not directly related to hardening.
Document default passwords: Documentation is useful, but changing or disabling default passwords is the hardening step.
Send server logs to the SIEM: Useful for monitoring and analysis but not a direct hardening step.
Join the server to the corporate domain: Part of integration into the network but not specific to hardening.

QUESTION 102
A company would like to provide employees with computers that do not have access to the internet in order to prevent information from being leaked to an online forum. Which of the following would be best for the systems administrator to implement?

A. Air gap
B. Jump server
C. Logical segmentation
D. Virtualization

Correct Answer: A
Section:
Explanation:
To provide employees with computers that do not have access to the internet and prevent information leaks to an online forum, implementing an air gap would be the best solution. An air gap physically isolates the computer or network from any outside connections, including the internet, ensuring that data cannot be transferred to or from the system.
Air gap: A security measure that isolates a computer or network from the internet or other networks, preventing any form of electronic communication with external systems.
Jump server: A secure server used to access and manage devices in a different security zone, but it does not provide isolation from the internet.
Logical segmentation: Segregates networks using software or network configurations, but it does not guarantee complete isolation from the internet.
Virtualization: Creates virtual instances of systems, which can be isolated, but does not inherently prevent internet access without additional configurations.

QUESTION 103
Which of the following penetration testing teams is focused only on trying to compromise an organization using an attacker's tactics?

A. White
B. Red
C. Purple
D. Blue

Correct Answer: B
Section:
Explanation:
Red teams are focused only on trying to compromise an organization using an attacker's tactics. They simulate real-world attacks to test the effectiveness of the organization's security defenses and identify vulnerabilities.
Red team: Acts as adversaries to simulate attacks and find security weaknesses.
White team: Oversees and ensures the rules of engagement are followed during the penetration test.
Purple team: Facilitates collaboration between the red team and the blue team to improve security.
Blue team: Defends against attacks and responds to security incidents.

QUESTION 104
Which of the following risks can be mitigated by HTTP headers?

A. SQLi
B. XSS
C. DoS
D. SSL

Correct Answer: B
Section:
Explanation:
HTTP headers can be used to mitigate risks associated with Cross-Site Scripting (XSS). Security-related HTTP headers such as Content Security Policy (CSP) and X-XSS-Protection can be configured to prevent the execution of malicious scripts in the context of a web page.
XSS (Cross-Site Scripting): A vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. HTTP headers like CSP help prevent XSS attacks by specifying which dynamic resources are allowed to load.
SQLi (SQL Injection): Typically mitigated by using parameterized queries and input validation, not HTTP headers.
DoS (Denial of Service): Mitigated by network and application-level defenses rather than HTTP headers.
SSL (Secure Sockets Layer): Refers to securing communications and is not directly mitigated by HTTP headers; rather, it's implemented using SSL/TLS protocols.

QUESTION 105
The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT
B. Insider threat
C. Data exfiltration
D. Service disruption

Correct Answer: A
Section:
Explanation:
The marketing department setting up its own project management software without informing the appropriate departments is an example of Shadow IT. Shadow IT refers to the use of IT systems, devices, software,

applications, and services without explicit approval from the IT department.
Shadow IT: Involves the use of unauthorized systems and applications within an organization, which can lead to security risks and compliance issues.
Insider threat: Refers to threats from individuals within the organization who may intentionally cause harm or misuse their access, but this scenario is more about unauthorized use rather than malicious intent.
Data exfiltration: Involves unauthorized transfer of data out of the organization, which is not the main issue in this scenario.
Service disruption: Refers to interruptions in service availability, which is not directly related to the marketing department's actions.

QUESTION 106
A network administrator is working on a project to deploy a load balancer in the company's cloud environment. Which of the following fundamental security requirements does this project fulfill?

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

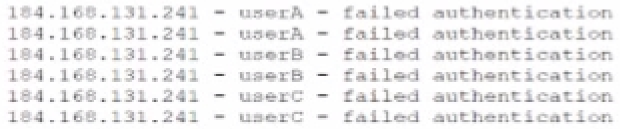
Correct Answer: D
Section:
Explanation:
Deploying a load balancer in the company's cloud environment primarily fulfills the fundamental security requirement of availability. A load balancer distributes incoming network traffic across multiple servers, ensuring that no single server becomes overwhelmed and that the service remains available even if some servers fail.
Availability: Ensures that services and resources are accessible when needed, which is directly supported by load balancing.
Privacy: Protects personal and sensitive information from unauthorized access but is not directly related to load balancing.
Integrity: Ensures that data is accurate and has not been tampered with, but load balancing is not primarily focused on data integrity.
Confidentiality: Ensures that information is accessible only to authorized individuals, which is not the primary concern of load balancing.

QUESTION 107
An external vendor recently visited a company's headquarters tor a presentation. Following the visit a member of the hosting team found a file that the external vendor left behind on a server. The file contained detailed architecture information and code snippets. Which of the following data types best describes this file?

A. Government
B. Public
C. Proprietary
D. Critical

Correct Answer: C
Section:
Explanation:
The file left by the external vendor, containing detailed architecture information and code snippets, is best described as proprietary data. Proprietary data is information that is owned by a company and is essential to its competitive advantage. It includes sensitive business information such as trade secrets, intellectual property, and confidential data that should be protected from unauthorized access.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of data classification and protection.

QUESTION 108
The security operations center is researching an event concerning a suspicious IP address A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced faded log-In attempts when authenticating from the same IP address:



```
184.168.131.241 - userA - failed authentication
184.168.131.241 - userA - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userC - failed authentication
184.168.131.241 - userC - failed authentication
```

Which of the following most likely describes attack that took place?

A. Spraying
B. Brute-force
C. Dictionary
D. Rainbow table

Correct Answer: A
Section:
Explanation:
Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for many user accounts from the same IP address are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

QUESTION 109
Which of the following explains why an attacker cannot easily decrypt passwords using a rainbow table attack?

A. Digital signatures
B. Salting
C. Hashing
D. Perfect forward secrecy

Correct Answer: B
Section:
Explanation:
Salting is a technique used to enhance the security of hashed passwords by adding a unique, random value (salt) to each password before hashing it. This prevents attackers from easily decrypting passwords using rainbow tables, which are precomputed tables for reversing cryptographic hash functions. Since each password has a unique salt, the same password will produce different hash values, making rainbow table attacks ineffective.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Hashing Techniques.

QUESTION 110
Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

A. SLA
B. MOU
C. MOA
D. BPA

Correct Answer: A
Section:
Explanation:
A Service Level Agreement (SLA) is a formal document between a service provider and a client that defines the expected level of service, including what resources will be provided and the agreed-upon time frames. It typically includes metrics to evaluate performance, uptime guarantees, and response times.
MOU (Memorandum of Understanding) and MOA (Memorandum of Agreement) are less formal and may not specify the exact level of service.
BPA (Business Partners Agreement) focuses more on the long-term relationship between partners.

QUESTION 111
Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?

A. Continuity of operations
B. Capacity planning
C. Tabletop exercise
D. Parallel processing

Correct Answer: C
Section:
Explanation:
A tabletop exercise involves the executive team or key stakeholders discussing and testing the company's incident response plan in a simulated environment. These exercises are low-stress, discussion-based, and help to validate the plan's effectiveness by walking through different scenarios without disrupting actual operations. It is an essential part of testing business continuity and incident response strategies.
Continuity of operations refers to the ability of an organization to continue functioning during and after a disaster but doesn't specifically involve simulations like tabletop exercises.
Capacity planning is related to ensuring the infrastructure can handle growth, not incident response testing.
Parallel processing refers to running multiple processes simultaneously, which is unrelated to testing an incident response plan.

QUESTION 112
Which of the following methods would most likely be used to identify legacy systems?

A. Bug bounty program
B. Vulnerability scan
C. Package monitoring
D. Dynamic analysis

Correct Answer: B
Section:
Explanation:

A vulnerability scan is the most likely method to identify legacy systems. These scans assess an organization's network and systems for known vulnerabilities, including outdated or unsupported software (i.e., legacy systems) that may pose a security risk. The scan results can highlight systems that are no longer receiving updates, helping IT teams address these risks.
Bug bounty programs are used to incentivize external researchers to find security flaws, but they are less effective at identifying legacy systems.
Package monitoring tracks installed software packages for updates or issues but is not as comprehensive for identifying legacy systems.
Dynamic analysis is typically used for testing applications during runtime to find vulnerabilities, but not for identifying legacy systems.

QUESTION 113
Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?

A. Reporting structure for the data privacy officer
B. Request process for data subject access
C. Role as controller or processor
D. Physical location of the company

Correct Answer: C
Section:
Explanation:
The most important consideration when establishing a data privacy program is defining the organization's role as a controller or processor. These roles, as outlined in privacy regulations such as the General Data Protection Regulation (GDPR), determine the responsibilities regarding the handling of personal data. A controller is responsible for determining the purpose and means of data processing, while a processor acts on behalf of the controller. This distinction is crucial for compliance with data privacy laws.
Reporting structure for the data privacy officer is important, but it is a secondary consideration compared to legal roles.
Request process for data subject access is essential for compliance but still depends on the organization's role as controller or processor.
Physical location of the company can affect jurisdiction, but the role as controller or processor has a broader and more immediate impact.

QUESTION 114

Client files can only be accessed by employees who need to know the information and have specified roles in the company. Which of the following best describes this security concept?

A. Availability
B. Confidentiality
C. Integrity
D. Non-repudiation

Correct Answer: B
Section:
Explanation:

The scenario described, where client files are only accessible to employees who 'need to know' the information, reflects the concept of confidentiality. Confidentiality ensures that sensitive information is only accessible to those who are authorized to view it, preventing unauthorized access.
Availability ensures that data is accessible when needed but doesn't focus on restricting access.
Integrity ensures that data remains accurate and unaltered but doesn't pertain to access control.
Non-repudiation ensures that actions cannot be denied after they are performed, but this concept is unrelated to access control.

QUESTION 115

A user would like to install software and features that are not available with a smartphone's default software. Which of the following would allow the user to install unauthorized software and enable new features?

A. SOU
B. Cross-site scripting
C. Jailbreaking
D. Side loading

Correct Answer: C
Section:
Explanation:

Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections.
SOU (Statement of Understanding) is not related to modifying devices.
Cross-site scripting is a web-based attack technique, unrelated to smartphone software.
Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

QUESTION 116

A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can Integrate easily into a user's workflow, and can utilize employee-owned devices. Which of the following will meet these requirements?

A. Push notifications
B. Phone call
C. Smart card
D. Offline backup codes

Correct Answer: A
Section:
Explanation:

Push notifications offer a seamless and user-friendly method of multi-factor authentication (MFA) that can easily integrate into a user's workflow. This method leverages employee-owned devices, like smartphones, to approve authentication requests through a push notification. It's convenient, quick, and doesn't require the user to input additional codes, making it a preferred choice for seamless integration with existing workflows.

Reference =
CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

QUESTION 117
A financial institution would like to store its customer data m the cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution Is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would best meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

Correct Answer: C
Section:
Explanation:
Homomorphic encryption allows data to be encrypted and manipulated without needing to decrypt it first. This cryptographic technique would allow the financial institution to store customer data securely in the cloud while still permitting operations like searching and calculations to be performed on the encrypted data. This ensures that the cloud service provider cannot decipher the sensitive data, meeting the institution's security requirements.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptographic Techniques.

QUESTION 118
The Chief Information Security Officer of an organization needs to ensure recovery from ransomware would likely occur within the organization's agreed-upon RPOs end RTOs. Which of the following backup scenarios would best ensure recovery?

A. Hourly differential backups stored on a local SAN array
B. Dally full backups stored on premises in magnetic offline media
C. Daly differential backups maintained by a third-party cloud provider
D. Weekly full backups with daily incremental stored on a NAS drive

Correct Answer: D
Section:
Explanation:
A backup strategy that combines weekly full backups with daily incremental backups stored on a NAS (Network Attached Storage) drive is likely to meet an organization's Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). This approach ensures that recent data is regularly backed up and that recovery can be done efficiently, without significant data loss or lengthy downtime.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Disaster Recovery and Backup Strategies.

QUESTION 119
Which of the following best describe a penetration test that resembles an actual external attach?

A. Known environment
B. Partially known environment
C. Bug bounty
D. Unknown environment

Correct Answer: D
Section:
Explanation:
An unknown environment in penetration testing, also known as a black-box test, simulates an actual external attack where the tester has no prior knowledge of the system. This type of penetration test is designed to mimic real-world attack scenarios, where an attacker has little to no information about the target environment. The tester must rely on various reconnaissance and attack techniques to uncover vulnerabilities, much like a real-world attacker would. This approach helps organizations understand their security posture from an external perspective, providing insights into how their defenses would hold up against a true outsider threat.
Reference =
CompTIA Security+ SY0-701 Course Content: The course highlights the importance of understanding different penetration testing environments, including black-box testing, which aligns with the 'unknown environment' in the provided answer.
CompTIA Security+ SY0-601 Study Guide: The guide details penetration testing methodologies, including black-box testing, which is crucial for simulating real external attacks.

QUESTION 120
A security team created a document that details the order in which critical systems should be through back online after a major outage. Which of the following documents did the team create?

A. Communication plan
B. Incident response plan
C. Data retention policy
D. Disaster recovery plan

Correct Answer: D
Section:
Explanation:
The document described in the question is a Disaster Recovery Plan (DRP). A DRP outlines the process and procedures for restoring critical systems and operations after a major disruption or outage. It includes the order in which systems should be brought back online to ensure minimal impact on business operations, prioritizing the most critical systems to recover first.
CompTIA Security+ SY0-701 Course Content: Domain 5: Security Program Management and Oversight, which discusses the development and implementation of disaster recovery plans.

QUESTION 121
Which of the following best represents an application that does not have an on-premises requirement and is accessible from anywhere?

A. Pass
B. Hybrid cloud
C. Private cloud
D. IaaS
E. SaaS

Correct Answer: E
Section:
Explanation:
Software as a Service (SaaS) represents an application that is hosted in the cloud and accessible via the internet from anywhere, with no requirement for on-premises infrastructure. SaaS applications are managed by a third-party provider, allowing users to access them through a web browser, making them highly scalable and flexible for remote access.
CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, where cloud service models such as SaaS are discussed, highlighting their accessibility and lack of on-premises requirements.

QUESTION 122
A company is utilizing an offshore team to help support the finance department. The company wants to keep the data secure by keeping it on a company device but does not want to provide equipment to the offshore team. Which of the following should the company implement to meet this requirement?

A. VDI
B. MDM

C. VPN
D. VPC

Correct Answer: A
Section:
Explanation:
Virtual Desktop Infrastructure (VDI) allows a company to host desktop environments on a centralized server. Offshore teams can access these virtual desktops remotely, ensuring that sensitive data stays within the company's infrastructure without the need to provide physical devices to the team. This solution is ideal for maintaining data security while enabling remote work, as all data processing occurs on the company's secure servers.
Reference =
CompTIA Security+ SY0-701 Course Content: VDI is discussed as a method for securely managing remote access to company resources without compromising data security.

QUESTION 123
The application development teams have been asked to answer the following questions:
* Does this application receive patches from an external source?
* Does this application contain open-source code?
* is this application accessible by external users?
* Does this application meet the corporate password standard?
Which of the following are these questions port of?

A. Risk control self-assessment
B. Risk management strategy
C. Risk acceptance
D. Risk matrix

Correct Answer: A
Section:
Explanation:
The questions listed are part of a Risk Control Self-Assessment (RCSA), which is a process where teams evaluate the risks associated with their operations and assess the effectiveness of existing controls. The questions focus on aspects such as patch management, the use of open-source code, external access, and compliance with corporate standards, all of which are critical for identifying and mitigating risks.
Reference =
CompTIA Security+ SY0-701 Course Content: The course discusses various risk management processes, including self-assessments that help in identifying and managing risks within the organization.

QUESTION 124
A security administrator is addressing an issue with a legacy system that communicates data using an unencrypted protocol to transfer sensitive data to a third party. No software updates that use an encrypted protocol are available, so a compensating control is needed. Which of the following are the most appropriate for the administrator to suggest? (Select two.)

A. Tokenization
B. Cryptographic downgrade
C. SSH tunneling
D. Segmentation
E. Patch installation
F. Data masking

Correct Answer: C, D
Section:
Explanation:

SSH tunneling can secure the unencrypted protocol by encapsulating traffic in an encrypted tunnel. Segmentation isolates the legacy system, reducing the risk of unauthorized access.

Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: 'Compensating Controls for Legacy Systems'.

QUESTION 125
An organization has a new regulatory requirement to implement corrective controls on a financial system. Which of the following is the most likely reason for the new requirement?

A. To defend against insider threats altering banking details
B. To ensure that errors are not passed to other systems
C. To allow for business insurance to be purchased
D. To prevent unauthorized changes to financial data

Correct Answer: D
Section:
Explanation:

Corrective controls, such as auditing and versioning, help prevent unauthorized changes to financial data, ensuring data integrity and compliance with regulations.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: 'Controls for Financial Systems'.

QUESTION 126
Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach affecting offshore offices. Which of the following is this an example of?

A. Tabletop exercise
B. Penetration test
C. Geographic dispersion
D. Incident response

Correct Answer: A
Section:
Explanation:

A tabletop exercise is a discussion-based activity where stakeholders simulate a security breach scenario to identify gaps in response plans and clarify roles and responsibilities.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: 'Incident Response Planning and Exercises'.

QUESTION 127
Which of the following is an example of a data protection strategy that uses tokenization?

A. Encrypting databases containing sensitive data
B. Replacing sensitive data with surrogate values
C. Removing sensitive data from production systems
D. Hashing sensitive data in critical systems

Correct Answer: B
Section:
Explanation:

Tokenization replaces sensitive data with non-sensitive surrogate values that retain the necessary format but are meaningless without access to the original data.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: 'Data Masking and Tokenization'..