

SY0-601 Dumps

CompTIA Security+ Exam

<https://www.certleader.com/SY0-601-dumps.html>



NEW QUESTION 1

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief Information Officer (CIO) believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

Answer: AE

NEW QUESTION 2

A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better.

- A. validate the vulnerability exists in the organization's network through penetration testing
- B. research the appropriate mitigation techniques in a vulnerability database
- C. find the software patches that are required to mitigate a vulnerability
- D. prioritize remediation of vulnerabilities based on the possible impact.

Answer: D

NEW QUESTION 3

An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

- A. Access to the organization's servers could be exposed to other cloud-provider clients
- B. The cloud vendor is a new attack vector within the supply chain
- C. Outsourcing the code development adds risk to the cloud provider
- D. Vendor support will cease when the hosting platforms reach EOL.

Answer: B

NEW QUESTION 4

Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should an administrator implement to protect the environment from this malware?

- A. Install a definition-based antivirus.
- B. Implement an IDS/IPS
- C. Implement a heuristic behavior-detection solution.
- D. Implement CASB to protect the network shares.

Answer: C

NEW QUESTION 5

A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before string. Which of the following techniques BEST explains this action?

- A. Predictability
- B. Key stretching
- C. Salting
- D. Hashing

Answer: C

NEW QUESTION 6

A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:

`http://dev-site.comptia.org/home/show.php?sessionID=77276554&loc=us`

The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

`http://dev-site.comptia.org/home/show.php?sessionID=98988475&loc=us` Which of the following application attacks is being tested?

- A. Pass-the-hash
- B. Session replay
- C. Object deference
- D. Cross-site request forgery

Answer: B

NEW QUESTION 7

A Chief Executive Officer (CEO) is dissatisfied with the level of service from the company's new service provider. The service provider is preventing the CEO from sending email from a work account to a personal account. Which of the following types of service

providers is being used?

- A. Telecommunications service provider
- B. Cloud service provider
- C. Master managed service provider
- D. Managed security service provider

Answer: B

NEW QUESTION 8

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

- A. A new firewall rule is needed to access the application.
- B. The system was quarantined for missing software updates.
- C. The software was not added to the application whitelist.
- D. The system was isolated from the network due to infected software.

Answer: C

NEW QUESTION 9

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen and later, enterprise data was found to have been compromised in a database. Which of the following was the MOST likely cause?

- A. Shadow IT
- B. Credential stuffing
- C. SQL injection
- D. Man-in-the-browser
- E. Bluejacking

Answer: A

NEW QUESTION 10

A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.
- The devices must be encrypted.
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

- A. Configuring an always-on VPN
- B. Implementing application whitelisting
- C. Requiring web traffic to pass through the on-premises content filter
- D. Setting the antivirus DAT update schedule to weekly

Answer: A

NEW QUESTION 10

The website <http://companywebsite.com> requires users to provide personal information, including security question responses, for registration. Which of the following would MOST likely cause a data breach?

- A. Lack of input validation
- B. Open permissions
- C. Unsecure protocol
- D. Missing patches

Answer: C

NEW QUESTION 12

A security analyst is reviewing the following command-line output:

```

Internet address      physical address      type
192.168.1.1          aa-bb-cc-00-11-22    dynamic
192.168.1.2          aa-bb-cc-00-11-22    dynamic
192.168.1.3          aa-bb-cc-00-11-22    dynamic
192.168.1.4          aa bb cc 00 11 22    dynamic
192.168.1.5          aa-bb-cc-00-11-22    dynamic
---output omitted---
--
192.168.1.251        aa-bb-cc-00-11-22    dynamic
192.168.1.252        aa bb cc 00 11 22    dynamic
192.168.1.253        aa-bb-cc-00-11-22    dynamic
192.168.1.254        aa-bb-cc-00-11-22    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static

```

Which of the following is the analyst observing?

- A. IGMP spoofing
- B. URL redirection
- C. MAC address cloning
- D. DNS poisoning

Answer: C

NEW QUESTION 17

Which of the following utilize a subset of real data and are MOST likely to be used to assess the features and functions of a system and how it interacts or performs from an end user's perspective against defined test cases? (Select TWO).

- A. Production
- B. Test
- C. Research and development
- D. PoC
- E. UAT
- F. SDLC

Answer: BE

NEW QUESTION 21

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine the next course of action?

- A. An incident response plan
- B. A communications plan
- C. A disaster recovery plan
- D. A business continuity plan

Answer: D

NEW QUESTION 23

A software developer needs to perform code-execution testing, black-box testing, and non-functional testing on a new product before its general release. Which of the following BEST describes the tasks the developer is conducting?

- A. Verification
- B. Validation
- C. Normalization
- D. Staging

Answer: A

NEW QUESTION 24

A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executives. Which of the following intelligence sources should the security analyst review?

- A. Vulnerability feeds
- B. Trusted automated exchange of indicator information
- C. Structured threat information expression
- D. Industry information-sharing and collaboration groups

Answer: D

NEW QUESTION 28

An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

- A. Require a complex, eight-character password that is updated every 90 days.
- B. Perform only non-intrusive scans of workstations.
- C. Use non-credentialed scans against high-risk servers.
- D. Log and alert on unusual scanner account logon times.

Answer: D

NEW QUESTION 29

A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

- A. Enforcing encryption
- B. Deploying GPOs
- C. Removing administrative permissions
- D. Applying MDM software

Answer: D

NEW QUESTION 30

A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

- A. Continuous delivery
- B. Continuous integration
- C. Continuous validation
- D. Continuous monitoring

Answer: B

NEW QUESTION 35

Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot access the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

- A. DDoS
- B. Man-in-the-middle
- C. MAC flooding
- D. Domain hijacking

Answer: A

NEW QUESTION 40

An organization that is located in a flood zone is MOST likely to document the concerns associated with the restoration of IT operation in a:

- A. business continuity plan
- B. communications plan.
- C. disaster recovery plan.
- D. continuity of operations plan

Answer: C

NEW QUESTION 44

A smart retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

* Protection from power outages

* Always-available connectivity in case of an outage

The owner has decided to implement battery backups for the computer equipment. Which of the following would BEST fulfill the owner's second need?

- A. Lease a point-to-point circuit to provide dedicated access.
- B. Connect the business router to its own dedicated UPS.
- C. Purchase services from a cloud provider for high availability.
- D. Replace the business's wired network with a wireless network.

Answer: C

NEW QUESTION 46

A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

- A. NIC teaming
- B. High availability
- C. Dual power supply
- D. IaaS

Answer: B

NEW QUESTION 48

A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

- A. Memory dumps
- B. The syslog server
- C. The application logs
- D. The log retention policy

Answer: B

NEW QUESTION 52

An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 am to 5:00 pm. Currently, the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the BEST way for the analyst to meet the business requirements?

- A. Incremental backups Monday through Friday at 6:00 p.m and differential backups hourly
- B. Full backups Monday through Friday at 6:00 p.m and incremental backups hourly.
- C. incremental backups Monday through Friday at 6:00 p.m and full backups hourly.
- D. Full backups Monday through Friday at 6:00 p.m and differential backups hourly.

Answer: A

NEW QUESTION 55

To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

- A. MaaS
- B. IaaS
- C. SaaS
- D. PaaS

Answer: D

NEW QUESTION 58

A network engineer notices the VPN concentrator overloaded and crashes on days when there are a lot of remote workers. Senior management has placed greater importance on the availability of VPN resources for the remote workers than the security of the end users' traffic. Which of the following would be BEST to solve this issue?

- A. IPsec
- B. Always On
- C. Split tunneling
- D. L2TP

Answer: B

NEW QUESTION 61

Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

- A. DLP
- B. HIDS
- C. EDR
- D. NIPS

Answer: C

NEW QUESTION 62

Given the following logs:

```
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "password"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "access"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "allow"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "please"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "ftp"
[ATTEMPT] target 192.168.50.1 - login "admin" - pass "letmein"
[21][ftp] host: 192.168.50.1 login:admin password:letmein
1 of 1 target successfully completed, 1 valid password found
```

Which of the following BEST describes the type of attack that is occurring?

- A. Rainbow table
- B. Dictionary
- C. Password spraying
- D. Pass-the-hash

Answer: C

NEW QUESTION 64

A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

- A. perform attribution to specific APTs and nation-state actors.
- B. anonymize any PII that is observed within the IoC data.
- C. add metadata to track the utilization of threat intelligence reports.
- D. assist companies with impact assessments based on the observed data.

Answer: B

NEW QUESTION 67

After entering a username and password, and administrator must gesture on a touch screen. Which of the following demonstrates what the administrator is providing?

- A. Multifactor authentication
- B. Something you can do
- C. Biometric
- D. Two-factor authentication

Answer: D

NEW QUESTION 72

A security analyst is investigating an incident to determine what an attacker was able to do on a compromised laptop. The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?

- A. An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack
- B. An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file
- C. An attacker was able to install malware to the CAasdf234 folder and use it to gain administrator rights and launch Outlook
- D. An attacker was able to phish user credentials successfully from an Outlook user profile

Answer: A

NEW QUESTION 73

A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

- A. Developing an incident response plan
- B. Building a disaster recovery plan
- C. Conducting a tabletop exercise
- D. Running a simulation exercise

Answer: C

NEW QUESTION 78

An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

- A. Voice
- B. Gait

- C. Vein
- D. Facial
- E. Retina
- F. Fingerprint

Answer: BD

NEW QUESTION 81

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS:

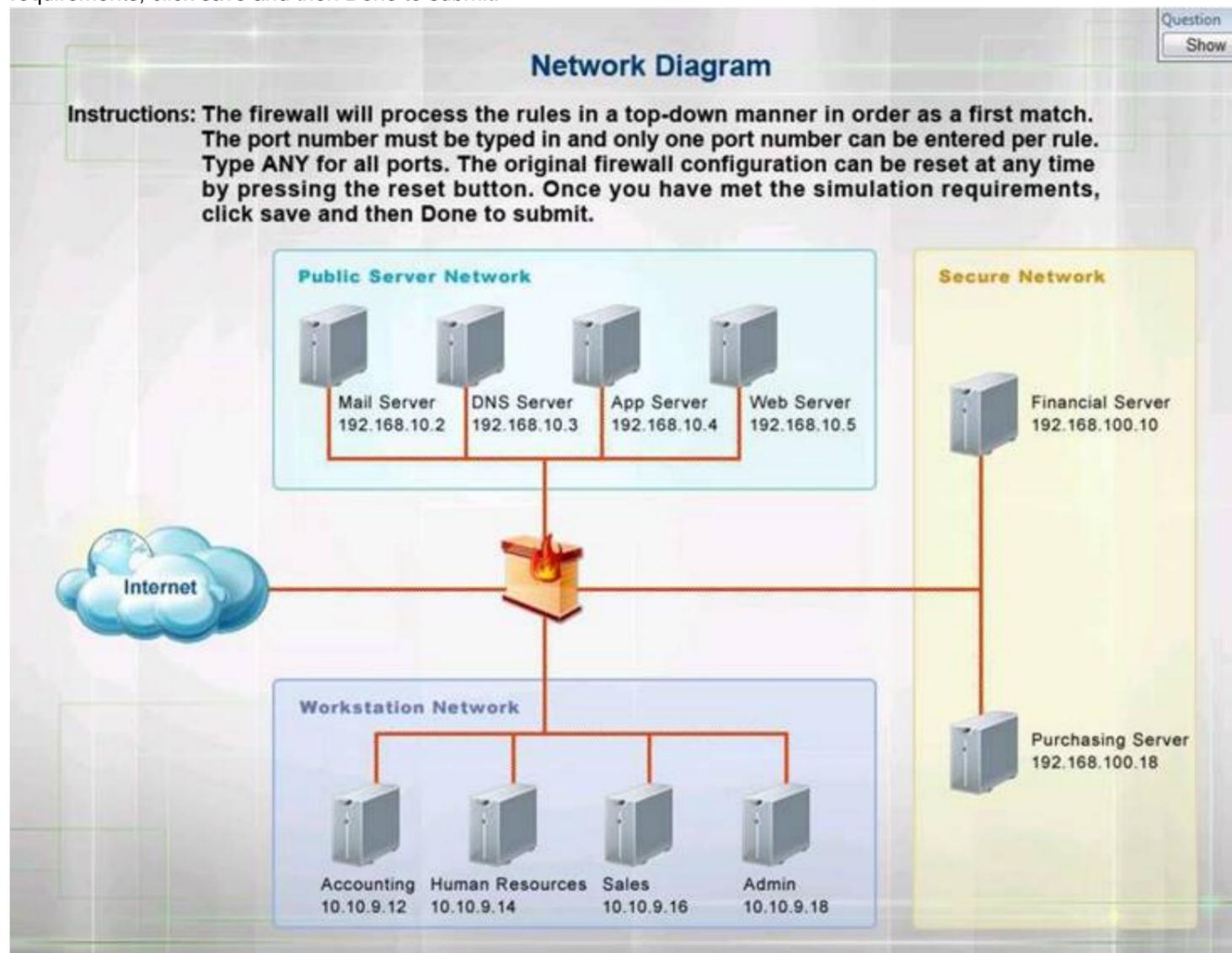
Click on the firewall and configure it to allow ONLY the following communication.

* 1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.

* 2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port

* 3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Hot Area:

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<ul style="list-style-type: none"> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32 	<ul style="list-style-type: none"> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32 	<ul style="list-style-type: none"> 443 22 69 	<ul style="list-style-type: none"> ANY TCP UDP 	<ul style="list-style-type: none"> Permit Deny
2	<ul style="list-style-type: none"> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32 	<ul style="list-style-type: none"> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32 	<ul style="list-style-type: none"> 443 22 69 	<ul style="list-style-type: none"> ANY TCP UDP 	<ul style="list-style-type: none"> Permit Deny
3	<ul style="list-style-type: none"> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32 	<ul style="list-style-type: none"> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32 	<ul style="list-style-type: none"> 443 22 69 	<ul style="list-style-type: none"> ANY TCP UDP 	<ul style="list-style-type: none"> Permit Deny
4	<ul style="list-style-type: none"> 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32 	<ul style="list-style-type: none"> Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32 	<ul style="list-style-type: none"> 443 22 69 	<ul style="list-style-type: none"> ANY TCP UDP 	<ul style="list-style-type: none"> Permit Deny

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated with medium confidence

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/32	22	TCP	Permit
3	10.10.9.18/32	192.168.100.10/32	69	ANY	Permit
4	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit

Graphical user interface Description automatically generated

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443. Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22. Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References: Stewart,

James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44 http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION 83

An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

- A. Order of volatility
- B. Data recovery
- C. Chain of custody
- D. Non-repudiation

Answer: C

NEW QUESTION 85

During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

- A. 1a
- B. chflags

- C. chmod
- D. leof
- E. setuid

Answer: D

NEW QUESTION 90

A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation. Which of the following would dispute the analyst's claim of innocence?

- A. Legal hold
- B. Order of volatility
- C. Non-repudiation
- D. Chain of custody

Answer: D

NEW QUESTION 95

A cloud administrator is configuring five compute instances under the same subnet in a VPC. Three instances are required to communicate with one another, and the other two must be logically isolated from all other instances in the VPC. Which of the following must the administrator configure to meet this requirement?

- A. One security group
- B. Two security groups
- C. Three security groups
- D. Five security groups

Answer: B

NEW QUESTION 98

A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

- A. Create DLP controls that prevent documents from leaving the network
- B. Implement salting and hashing
- C. Configure the web content filter to block access to the forum.
- D. Increase password complexity requirements

Answer: A

NEW QUESTION 103

Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

- A. Unsecure protocols
- B. Use of penetration-testing utilities
- C. Weak passwords
- D. Included third-party libraries
- E. Vendors/supply chain
- F. Outdated anti-malware software

Answer: AD

NEW QUESTION 105

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

Answer: BF

NEW QUESTION 110

During an incident response, a security analyst observes the following log entry on the web server. Which of the following BEST describes the type of attack the analyst is experiencing?

- A. SQL injection
- B. Cross-site scripting
- C. Pass-the-hash
- D. Directory traversal

Answer: B

NEW QUESTION 111

Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

- A. SaaS
- B. PaaS
- C. IaaS
- D. DaaS

Answer: C

NEW QUESTION 112

A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

- A. PCI DSS
- B. GDPR
- C. NIST
- D. ISO 31000

Answer: B

NEW QUESTION 116

A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

- A. The DNS logs
- B. The web server logs
- C. The SIP traffic logs
- D. The SNMP logs

Answer: A

NEW QUESTION 121

A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive. All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

- A. # iptables -t mangle -X
- B. # iptables -F
- C. # iptables -Z
- D. # iptables -P INPUT -j DROP

Answer: D

NEW QUESTION 126

Which of the following is a reason why an organization would define an AUP?

- A. To define the lowest level of privileges needed for access and use of the organization's resources
- B. To define the set of rules and behaviors for users of the organization's IT systems
- C. To define the intended partnership between two organizations
- D. To define the availability and reliability characteristics between an IT provider and consumer

Answer: B

NEW QUESTION 127

A security analyst is performing a forensic investigation compromised account credentials. Using the Event Viewer, the analyst able to detect the following message, "Special privileges assigned to new login." Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

- A. Pass-the-hash
- B. Buffer overflow
- C. Cross-site scripting
- D. Session replay

Answer: A

NEW QUESTION 131

Accompany deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

- A. WPA3
- B. AES
- C. RADIUS
- D. WPS

Answer:

D

NEW QUESTION 133

A company recently moved sensitive videos between on-premises. Company-owned websites. The company then learned the videos had been uploaded and shared to the internet. Which of the following would MOST likely allow the company to find the cause?

- A. Checksums
- B. Watermarks
- C. Oder of volatility
- D. A log analysis
- E. A right-to-audit clause

Answer: D

NEW QUESTION 134

A company was recently breached Part of the company's new cybersecurity strategy is to centralize the logs from all security devices Which of the following components forwards the logs to a central source?

- A. Log enrichment
- B. Log aggregation
- C. Log parser
- D. Log collector

Answer: D

NEW QUESTION 138

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- Check-in/checkout of credentials
- The ability to use but not know the password
- Automated password changes
- Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

Answer: D

NEW QUESTION 140

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

- A. Credential harvesting
- B. Keylogger
- C. Brute-force
- D. Spraying

Answer: D

NEW QUESTION 142

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

- A. Perform a site survey
- B. Deploy an FTK Imager
- C. Create a heat map
- D. Scan for rogue access points
- E. Upgrade the security protocols
- F. Install a captive portal

Answer: AC

NEW QUESTION 144

An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

- A. HSM
- B. CASB
- C. TPM
- D. DLP

Answer: A

NEW QUESTION 145

A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

- A. An air gap
- B. A Faraday cage
- C. A shielded cable
- D. A demilitarized zone

Answer: A

NEW QUESTION 146

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent the exfiltration of data? (Select TWO).

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File level encryption
- E. USB blocker
- F. MFA

Answer: BE

NEW QUESTION 147

A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

- A. SIEM
- B. DLP
- C. CASB
- D. SWG

Answer: C

NEW QUESTION 151

Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:

- There must be visibility into how teams are using cloud-based services.
- The company must be able to identify when data related to payment cards is being sent to the cloud.
- Data must be available regardless of the end user's geographic location
- Administrators need a single pane-of-glass view into traffic and trends. Which of the following should the security analyst recommend?

- A. Create firewall rules to restrict traffic to other cloud service providers.
- B. Install a DLP solution to monitor data in transit.
- C. Implement a CASB solution.
- D. Configure a web-based content filter.

Answer: B

NEW QUESTION 154

An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

- A. Document the collection and require a sign-off when possession changes.
- B. Lock the device in a safe or other secure location to prevent theft or alteration.
- C. Place the device in a Faraday cage to prevent corruption of the data.
- D. Record the collection in a blockchain-protected public ledger.

Answer: A

NEW QUESTION 159

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned that servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135

- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

Answer: AE

NEW QUESTION 160

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

Answer: C

NEW QUESTION 161

A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location Which of the following would BEST meet the architect's objectives?

- A. Trusted Platform Module
- B. IaaS
- C. HSMaaS
- D. PaaS
- E. Key Management Service

Answer: A

NEW QUESTION 165

An organization that has a large number of mobile devices is exploring enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more than 3mi (4.8km) from the building, the management team would like to have the security team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?

- A. Geofencing
- B. Lockout
- C. Near-field communication
- D. GPS tagging

Answer: A

NEW QUESTION 168

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

- A. Bug bounty
- B. Black-box
- C. Gray-box
- D. White-box

Answer: A

NEW QUESTION 170

A network technician is installing a guest wireless network at a coffee shop. When a customer purchases an item, the password for the wireless network is printed on the receipt so the customer can log in. Which of the following will the technician MOST likely configure to provide the highest level of security with the least amount of overhead?

- A. WPA-EAP
- B. WEP-TKIP
- C. WPA-PSK
- D. WPS-PIN

Answer: A

NEW QUESTION 173

Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

- A. SIEM
- B. CASB
- C. UTM
- D. DLP

Answer: D

NEW QUESTION 176

Which of the following will MOST likely cause machine learning and AI-enabled systems to operate with unintended consequences?

- A. Stored procedures
- B. Buffer overflows
- C. Data bias
- D. Code reuse

Answer: A

Explanation:

<https://lionbridge.ai/articles/7-types-of-data-bias-in-machine-learning/>

NEW QUESTION 181

After installing a Windows server, a cybersecurity administrator needs to harden it, following security best practices. Which of the following will achieve the administrator's goal? (Select TWO).

- A. Disabling guest accounts
- B. Disabling service accounts
- C. Enabling network sharing
- D. Disabling NetBIOS over TCP/IP
- E. Storing LAN manager hash values
- F. Enabling NTLM

Answer: AD

NEW QUESTION 184

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

- A. An incident response plan
- B. A communications plan
- C. A business continuity plan
- D. A disaster recovery plan

Answer: A

NEW QUESTION 187

A Chief Security Officer (CSO) is concerned about the amount of PII that is stored locally on each salesperson's laptop. The sales department has a higher-than-average rate of lost equipment. Which of the following recommendations would BEST address the CSO's concern?

- A. Deploy an MDM solution.
- B. Implement managed FDE.
- C. Replace all hard drives with SEDs.
- D. Install DLP agents on each laptop.

Answer: B

NEW QUESTION 189

Which of the following algorithms has the SMALLEST key size?

- A. DES
- B. Twofish
- C. RSA
- D. AES

Answer: B

NEW QUESTION 193

A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

- A. An NGFW
- B. A CASB
- C. Application whitelisting
- D. An NG-SWG

Answer: B

NEW QUESTION 194

A security analyst is reviewing a penetration-testing report from a third-party contractor. The penetration testers used the organization's new API to bypass a driver to perform privilege escalation on the

organization's web servers. Upon looking at the API, the security analyst realizes the particular API call was to a legacy system running an outdated OS. Which of the following is the MOST likely attack type?

- A. Request forgery
- B. Session replay
- C. DLL injection
- D. Shimming

Answer: A

NEW QUESTION 195

Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

- A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords.
- B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server.
- C. Malware trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
- D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites

Answer: D

NEW QUESTION 198

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

- A. The vulnerability scan output
- B. The IDS logs
- C. The full packet capture data
- D. The SIEM alerts

Answer: A

NEW QUESTION 203

A security analyst needs to generate a server certificate to be used for 802.1X and secure RDP connections. The analyst is unsure what is required to perform the task and solicits help from a senior colleague. Which of the following is the FIRST step the senior colleague will most likely tell the analyst to perform to accomplish this task?

- A. Create an OCSP
- B. Generate a CSR
- C. Create a CRL
- D. Generate a .pfx file

Answer: B

NEW QUESTION 208

Which of the following control sets should a well-written BCP include? (Select THREE)

- A. Preventive
- B. Detective
- C. Deterrent
- D. Corrective
- E. Compensating
- F. Physical
- G. Recovery

Answer: ADG

NEW QUESTION 209

Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

- A. Staging
- B. Test
- C. Production
- D. Development

Answer: B

NEW QUESTION 210

A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

- A. DNSSEC
- B. Reverse proxy
- C. VPN concentrator
- D. PKI

- E. Active Directory
- F. RADIUS

Answer: EF

NEW QUESTION 213

A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

- A. Corrective
- B. Physical
- C. Detective
- D. Administrative

Answer: C

NEW QUESTION 217

In which of the following common use cases would steganography be employed?

- A. Obfuscation
- B. Integrity
- C. Non-repudiation
- D. Blockchain

Answer: A

NEW QUESTION 221

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

- A. Unsecured root accounts
- B. Zero day
- C. Shared tenancy
- D. Insider threat

Answer: C

NEW QUESTION 225

An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:

```
Hello everyone,  
I am having the same problem with my server. Can you help me?  
  
<script type="text/javascript" src=http://website.com/user.js>  
Onload=sqlexec();  
</script>  
  
Thank you,  
  
Joe
```

Which of the following BEST describes the attack that was attempted against the forum readers?

- A. SOU attack
- B. DLL attack
- C. XSS attack
- D. API attack

Answer: C

NEW QUESTION 227

Which of the following allows for functional test data to be used in new systems for testing and training purposes to protect the read data?

- A. Data encryption
- B. Data masking
- C. Data deduplication
- D. Data minimization

Answer: B

NEW QUESTION 231

The process of passively gathering information prior to launching a cyberattack is called:

- A. tailgating
- B. reconnaissance
- C. pharming
- D. prepending

Answer: B

NEW QUESTION 234

A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

- A. Mobile device management
- B. Full-device encryption
- C. Remote wipe
- D. Biometrics

Answer: A

NEW QUESTION 237

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

- A. SLA
- B. BPA
- C. NDA
- D. MOU

Answer: A

NEW QUESTION 241

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

- A. Configure the DLP policies to allow all PII
- B. Configure the firewall to allow all ports that are used by this application
- C. Configure the antivirus software to allow the application
- D. Configure the DLP policies to whitelist this application with the specific PII
- E. Configure the application to encrypt the PII

Answer: D

NEW QUESTION 242

A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

- A. The GPS location
- B. When the file was deleted
- C. The total number of print jobs
- D. The number of copies made

Answer: A

NEW QUESTION 245

A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a projected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

- A. DNS sinkholding
- B. DLP rules on the terminal
- C. An IP blacklist
- D. Application whitelisting

Answer: D

NEW QUESTION 247

An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

- A. Screen locks
- B. Application management
- C. Geofencing
- D. Containerization

Answer: D

NEW QUESTION 249

An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfer the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

- A. Nmap
- B. cURL
- C. Netcat

D. Wireshark

Answer: D

NEW QUESTION 250

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

- A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
- B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
- C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
- D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

Answer: C

NEW QUESTION 253

An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE)

- A. SFTP, FTPS
- B. SNMPv2, SNMPv3
- C. HTTP, HTTPS
- D. TFTP, FTP
- E. SNMPv1, SNMPv2
- F. Telnet, SSH
- G. TLS, SSL
- H. POP, IMAP
- I. Login, rlogin

Answer: BCF

NEW QUESTION 257

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key
- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

Answer: BC

NEW QUESTION 259

The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

- A. A script kiddie
- B. Shadow IT
- C. Hacktivism
- D. White-hat

Answer: B

NEW QUESTION 262

A security analyst is preparing a threat for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

- A. A table exercise
- B. NST CSF
- C. MTRE ATT\$CK
- D. OWASP

Answer: C

NEW QUESTION 266

A security engineer has enabled two-factor authentication on all workstations. Which of the following approaches are the MOST secure? (Select TWO).

- A. Password and security question
- B. Password and CAPTCHA
- C. Password and smart card
- D. Password and fingerprint
- E. Password and one-time token
- F. Password and voice

Answer: CD

NEW QUESTION 269

Which of the following types of controls is a turnstile?

- A. Physical
- B. Detective
- C. Corrective
- D. Technical

Answer: A

NEW QUESTION 274

A user recently entered a username and password into a recruiting application website that had been forged to look like the legitimate site. Upon investigation, a security analyst identifies the following:

- The legitimate website's IP address is 10.1.1.20 and eRecruit local resolves to the IP
 - The forged website's IP address appears to be 10.2.12.99, based on NetFlow records
 - AH three at the organization's DNS servers show the website correctly resolves to the legitimate IP
 - DNS query logs show one of the three DNS servers returned a result of 10.2.12.99 (cached) at the approximate time of the suspected compromise.
- Which of the following MOST likely occurred?

- A. A reverse proxy was used to redirect network traffic
- B. An SSL strip MITM attack was performed
- C. An attacker temporarily pawned a name server
- D. An ARP poisoning attack was successfully executed

Answer: B

NEW QUESTION 276

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

Answer: B

NEW QUESTION 278

An attacker is exploiting a vulnerability that does not have a patch available. Which of the following is the attacker exploiting?

- A. Zero-day
- B. Default permissions
- C. Weak encryption
- D. Unsecure root accounts

Answer: A

NEW QUESTION 282

A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent data? (Select TWO)

- A. VPN
- B. Drive encryption
- C. Network firewall
- D. File-level encryption
- E. USB blocker
- F. MFA

Answer: BE

NEW QUESTION 285

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operation in the event of a prolonged DDoS attack on its local datacenter that consumes database resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

- A. Upgrade the bandwidth available into the datacenter
- B. Implement a hot-site failover location
- C. Switch to a complete SaaS offering to customers
- D. Implement a challenge response test on all end-user queries

Answer: B

NEW QUESTION 288

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

- A. Hping3 -s comptia.org -p 80
- B. Nc -1 -v comptia.org -p 80
- C. nmap comptia.org -p 80 -aV
- D. nslookup -port=80 comptia.org

Answer: C

NEW QUESTION 292

A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicates a directory-traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A)

```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B)

```
http://sample.url.com/someotherpageonsite/../../../../etc/shadow
```

C)

```
http://sample.url.com/select-from-database-where-password-null
```

D)

```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 293

Users have been issued smart cards that provide physical access to a building. The cards also contain tokens that can be used to access information systems. Users can log in to any thin client located throughout the building and see the same desktop each time. Which of the following technologies are being utilized to provide these capabilities? (Select TWO)

- A. COPE
- B. VDI
- C. GPS
- D. TOTP
- E. RFID
- F. BYOD

Answer: BE

NEW QUESTION 297

A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess its security.

Strategy for mitigating risks within the perimeter Which of the following solutions would BEST support the organization's strategy?

- A. FIM
- B. DLP
- C. EDR
- D. UTM

Answer: C

NEW QUESTION 300

Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO).

- A. Testing security systems and processes regularly
- B. Installing and maintaining a web proxy to protect cardholder data
- C. Assigning a unique ID to each person with computer access
- D. Encrypting transmission of cardholder data across private networks
- E. Benchmarking security awareness training for contractors
- F. Using vendor-supplied default passwords for system passwords

Answer: BD

NEW QUESTION 305

A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

- A. PCI DSS
- B. ISO 22301
- C. ISO 27001
- D. NIST CSF

Answer: A

NEW QUESTION 307

A Chief Security Officer (CSO) was notified that a customer was able to access confidential internal company files on a commonly used file-sharing service. The file-sharing service is the same one used by company staff as one of its approved third-party applications.

After further investigation, the security team determines the sharing of confidential files was accidental and not malicious. However, the CSO wants to implement changes to minimize this type of incident from reoccurring but does not want to impact existing business processes. Which of the following would BEST meet the CSO's objectives?

- A. DLP
- B. SWG
- C. CASB
- D. Virtual network segmentation
- E. Container security

Answer: A

NEW QUESTION 310

Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

- A. Integer overflow
- B. Zero-day
- C. End of life
- D. Race condition

Answer: B

NEW QUESTION 311

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

- A. SSAE SOC 2
- B. PCI DSS
- C. GDPR
- D. ISO 31000

Answer: C

NEW QUESTION 313

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

- A. A RAT was installed and is transferring additional exploit tools.
- B. The workstations are beaconing to a command-and-control server.
- C. A logic bomb was executed and is responsible for the data transfers.
- D. A fileless virus is spreading in the local network environment.

Answer: A

NEW QUESTION 318

In the middle of a cybersecurity, a security engineer removes the infected devices from the network and lock down all compromised accounts. In which of the following incident response phases is the security engineer currently operating?

- A. Identification
- B. Preparation
- C. Eradiction
- D. Recovery
- E. Containment

Answer: E

NEW QUESTION 322

Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

- A. A right-to-audit clause allowing for annual security audits
- B. Requirements for event logs to be kept for a minimum of 30 days
- C. Integration of threat intelligence in the company's AV

D. A data-breach clause requiring disclosure of significant data loss

Answer: A

NEW QUESTION 327

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

Answer: A

NEW QUESTION 330

On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.)

- A. Data accessibility
- B. Legal hold
- C. Cryptographic or hash algorithm
- D. Data retention legislation
- E. Value and volatility of data
- F. Right-to-audit clauses

Answer: EF

NEW QUESTION 331

A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

- A. OAuth
- B. SSO
- C. SAML
- D. PAP

Answer: C

NEW QUESTION 336

An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the Incident could have been prevented?

- A. The vulnerability scan output
- B. The security logs
- C. The baseline report
- D. The correlation of events

Answer: A

NEW QUESTION 341

When selecting a technical solution for identity management, an architect chooses to go from an in-house to a third-party SaaS provider. Which of the following risk management strategies is this an example of?

- A. Acceptance
- B. Mitigation
- C. Avoidance
- D. Transference

Answer: D

NEW QUESTION 344

A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.)

- A. Trusted Platform Module
- B. A host-based firewall
- C. A DLP solution
- D. Full disk encryption
- E. A VPN
- F. Antivirus software

Answer: AB

NEW QUESTION 348

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. When of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. AVLAN
- D. A screened subnet

Answer: D

NEW QUESTION 350

Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function properly. Which of the following should the security administrator consider implementing to address this issue?

- A. Application code signing
- B. Application whitelisting
- C. Data loss prevention
- D. Web application firewalls

Answer: B

NEW QUESTION 353

An organization recently recovered from a data breach. During the root cause analysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

- A. MDM
- B. MAM
- C. VDI
- D. DLP

Answer: A

NEW QUESTION 358

A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is MOST likely the cause?

- A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.
- B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
- C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
- D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Answer: D

NEW QUESTION 361

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:

- * Employees must provide an alternate work location (i.e., a home address)
- * Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

- A. Geofencing, content management, remote wipe, containerization, and storage segmentation
- B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
- C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
- D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

Answer: D

NEW QUESTION 365

Joe, an employee, is transferring departments and is providing copies of his files to a network share folder for his previous team to access. Joe is granting read-write-execute permissions to his manager but giving read-only access to the rest of the team. Which of the following access controls is Joe using?

- A. ACL
- B. DAC
- C. ABAC
- D. MAC

Answer: D

NEW QUESTION 366

A company's Chief Information Office (CIO) is meeting with the Chief Information Security Officer (CISO) to plan some activities to enhance the skill levels of the company's developers. Which of the following would be MOST suitable for training the developers'?

- A. A capture-the-flag competition
- B. A phishing simulation
- C. Physical security training
- D. Baste awareness training

Answer: B

NEW QUESTION 369

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

- A. Security
- B. Application
- C. Dump
- D. Syslog

Answer: C

NEW QUESTION 370

A worldwide manufacturing company has been experiencing email account compromised. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

- A. Network location
- B. Impossible travel time
- C. Geolocation
- D. Geofencing

Answer: D

NEW QUESTION 373

Which of the following is a team of people dedicated testing the effectiveness of organizational security programs by emulating the techniques of potential attackers?

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

Answer: A

NEW QUESTION 376

A company is designing the layout of a new datacenter so it will have an optimal environmental temperature. Which of the following must be included? (Select TWO)

- A. An air gap
- B. A cold aisle
- C. Removable doors
- D. A hot aisle
- E. An IoT thermostat
- F. A humidity monitor

Answer: EF

NEW QUESTION 378

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN? (Select TWO).

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest patch update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.
- E. The laptop is still configured to connect to an international mobile network operator.
- F. The user is unable to authenticate because they are outside of the organization's mobile geofencing configuration.

Answer: AB

NEW QUESTION 382

An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

- A. The baseline
- B. The endpoint configurations
- C. The adversary behavior profiles
- D. The IPS signatures

Answer: C

NEW QUESTION 384

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the

legitimate access ports Which of the following attacks is happening on the corporate network?

- A. Man in the middle
- B. Evil twin
- C. Jamming
- D. Rogue access point
- E. Disassociation

Answer: B

NEW QUESTION 389

A security engineer needs to implement the following requirements:

- All Layer 2 switches should leverage Active Directory for authentication.
- All Layer 2 switches should use local fallback authentication if Active Directory is offline.
- All Layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

- A. Implement RADIUS.
- B. Configure AAA on the switch with local login as secondary.
- C. Configure port security on the switch with the secondary login method.
- D. Implement TACACS+.
- E. Enable the local firewall on the Active Directory server.
- F. Implement a DHCP server.

Answer: AB

NEW QUESTION 393

After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

Answer: C

NEW QUESTION 396

A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

- A. A firewall
- B. A device pin
- C. A USB data blocker
- D. Biometrics

Answer: C

NEW QUESTION 400

A company has limited storage available and online presence that cannot for more than four hours. Which of the following backup methodologies should the company implement to allow for the FASTEST database restore time in the event of a failure, while being mindful of the limited available storage space?

- A. Implement fulltape backup every Sunday at 8:00 p.m. and perform nightly tape rotations.
- B. Implement differential backups every Sunday at 8:00 and nightly incremental backups at 8:00 p.m.
- C. Implement nightly full backups every Sunday at 8:00 p.m.
- D. Implement full backups every Sunday at 8:00 p.m. and nightly differential backups at 8:00

Answer: B

NEW QUESTION 405

To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

- A. PFS
- B. SPF
- C. DMARC
- D. DNSSEC

Answer: D

NEW QUESTION 407

Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

- A. Cameras
- B. Faraday cage
- C. Access control vestibule

- D. Sensors
- E. Guards

Answer: C

NEW QUESTION 412

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

Answer: C

NEW QUESTION 417

A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words. Which of the following would be the BEST to use?

- A. IDS solution
- B. EDR solution
- C. HIPS software solution
- D. Network DLP solution

Answer: D

NEW QUESTION 418

A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

- A. Due to foreign travel, the user's laptop was isolated from the network.
- B. The user's laptop was quarantined because it missed the latest patch update.
- C. The VPN client was blacklisted.
- D. The user's account was put on a legal hold.

Answer: A

NEW QUESTION 423

A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

- A. 1
- B. 5
- C. 6

Answer: B

NEW QUESTION 424

A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

- A. OSINT
- B. SIEM
- C. CVSS
- D. CVE

Answer: D

NEW QUESTION 429

A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following scan types would produce the BEST vulnerability scan report?

- A. Port
- B. Intrusive
- C. Host discovery
- D. Credentialed

Answer: D

NEW QUESTION 431

An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

- A. TLS

- B. PFS
- C. ESP
- D. AH

Answer: A

NEW QUESTION 434

The new Chief Executive Officer (CEO) of a large company has announced a partnership with a vendor that will provide multiple collaboration applications to make remote work easier. The company has a geographically dispersed staff located in numerous remote offices in different countries. The company's IT administrators are concerned about network traffic and load if all users simultaneously download the application. Which of the following would work BEST to allow each geographic region to download the software without negatively impacting the corporate network?

- A. Update the host IDS rules.
- B. Enable application whitelisting.
- C. Modify the corporate firewall rules.
- D. Deploy all applications simultaneously.

Answer: B

NEW QUESTION 436

The human resources department of a large online retailer has received multiple customer complaints about the rudeness of the automated chatbots it uses to interface and assist online shoppers. The system, which continuously learns and adapts, was working fine when it was installed a few months ago. Which of the following BEST describes the method being used to exploit the system?

- A. Baseline modification
- B. A fileless virus
- C. Tainted training data
- D. Cryptographic manipulation

Answer: C

NEW QUESTION 437

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

- A. Fileless malware
- B. A downgrade attack
- C. A supply-chain attack
- D. A logic bomb
- E. Misconfigured BIOS

Answer: C

NEW QUESTION 440

A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted. Which of the following resiliency techniques was applied to the network to prevent this attack?

- A. NIC Teaming
- B. Port mirroring
- C. Defense in depth
- D. High availability
- E. Geographic dispersal

Answer: C

NEW QUESTION 441

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system updates automatically.

Answer: A

NEW QUESTION 445

Which of the following scenarios BEST describes a risk reduction technique?

- A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
- B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
- C. A security control objective cannot be met through a technical change, so the company changes its method of operation.
- D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

Answer: B

NEW QUESTION 447

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization MOST likely consult?

- A. The business continuity plan
- B. The disaster recovery plan
- C. The communications plan
- D. The incident response plan

Answer: A

NEW QUESTION 452

A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authenticate the entire packet?

- A. AH
- B. ESP
- C. SRTP
- D. LDAP

Answer: B

NEW QUESTION 456

The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

- A. Limit the use of third-party libraries.
- B. Prevent data exposure queries.
- C. Obfuscate the source code.
- D. Submit the application to QA before releasing it.

Answer: D

NEW QUESTION 459

A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

- A. MAC
- B. ACL
- C. BPDU
- D. ARP

Answer: A

NEW QUESTION 463

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the BEST options to accomplish this objective? (Select TWO)

- A. Load balancing
- B. Incremental backups
- C. UPS
- D. RAID
- E. Dual power supply
- F. NIC teaming

Answer: AD

NEW QUESTION 465

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-601 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SY0-601-dumps.html>