

# CompTIA

## Exam Questions SY0-601

CompTIA Security+ Exam



**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 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 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**

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 3**

A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

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

**Answer:** D

**NEW QUESTION 4**

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 5**

The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

- A. federation.
- B. a remote access policy.
- C. multifactor authentication.
- D. single sign-on.

**Answer:** D

**NEW QUESTION 6**

An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: `ipconfig /flushdns`, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

- A. DNS cache poisoning
- B. Domain hijacking
- C. Distributed denial-of-service
- D. DNS tunneling

**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

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 9

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 cause of the access issues?

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

**Answer: B**

#### NEW QUESTION 10

A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

- A. Payment Card Industry Data Security Standard
- B. Cloud Security Alliance Best Practices
- C. ISO/IEC 27032 Cybersecurity Guidelines
- D. General Data Protection Regulation

**Answer: A**

#### NEW QUESTION 10

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 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 14

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 19

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 22**

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 24**

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 26**

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 30**

A network administrator has been asked to design a solution to improve a company's security posture. The administrator is given the following requirements:

- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

- A. HIDS
- B. NIDS
- C. HIPS
- D. NIPS

**Answer: D**

**NEW QUESTION 35**

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 36**

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 38**

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 42**

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 47**

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 51**

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 54**

Which of the following would be BEST to establish between organizations that have agreed cooperate and are engaged in early discussion to define the responsibilities of each party, but do not want to establish a contractually binding agreement?

- A. An SLA
- B. AnNDA
- C. ABPA
- D. AnMOU

**Answer:** D

**NEW QUESTION 57**

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

- A. STIX
- B. CIRT
- C. OSINT
- D. TAXII

**Answer:** B

**NEW QUESTION 61**

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 64**

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:

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 65**

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 70**

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 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:

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 76

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 79

An incident, which is affecting dozens of systems, involves malware that reaches out to an Internet service for rules and updates. The IP addresses for the Internet host appear to be different in each case. The organization would like to determine a common IoC to support response and recovery actions. Which of the following sources of information would BEST support this solution?

- A. Web log files
- B. Browser cache
- C. DNS query logs
- D. Antivirus

**Answer: C**

#### NEW QUESTION 82

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 83

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 87

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 91

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 94**

A user recently attended an exposition and received some digital promotional materials. The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open. Which of the following is MOST likely the cause of the reported issue?

- A. There was a drive-by download of malware
- B. The user installed a cryptominer
- C. The OS was corrupted
- D. There was malicious code on the USB drive

**Answer:** D

**NEW QUESTION 99**

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

- A. An external security assessment
- B. A bug bounty program
- C. A tabletop exercise
- D. A red-team engagement

**Answer:** C

**NEW QUESTION 100**

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going to the polls. This is an example of:

- A. prepending.
- B. an influence campaign
- C. a watering-hole attack
- D. intimidation
- E. information elicitation

**Answer:** D

**NEW QUESTION 104**

Joe, a security analyst, recently performed a network discovery to fully understand his organization's electronic footprint from a "public" perspective. Joe ran a set of commands and received the following output:

Which of the following can be determined about the organization's public presence and security posture? (Select TWO).

- A. Joe used Whois to produce this output.
- B. Joe used cURL to produce this output.
- C. Joe used Wireshark to produce this output.
- D. The organization has adequate information available in public registration.
- E. The organization has too much information available in public registration.
- F. The organization has too little information available in public registration.

**Answer:** AD

**NEW QUESTION 109**

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 111**

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 115**



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 118

A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

#### NEW QUESTION 119

A security administrator needs to create a RAIS configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drivers will fail simultaneously. Which of the following RAID configurations should the administration use?

- A. RA1D 0
- B. RAID1
- C. RAID 5
- D. RAID 10

**Answer:** C

#### NEW QUESTION 120

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

Which of the following can the security analyst conclude?

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

**Answer:** C

#### NEW QUESTION 125

A smart switch has the ability to monitor electrical levels and shut off power to a building in the event of power surge or other fault situation. The switch was installed on a wired network in a hospital and is monitored by the facilities department via a cloud application. The security administrator isolated the switch on a separate VLAN and set up a patch routine. Which of the following steps should also be taken to harden the smart switch?

- A. Set up an air gap for the switch.
- B. Change the default password for the switch.
- C. Place the switch In a Faraday cage.
- D. Install a cable lock on the switch

**Answer: B**

**NEW QUESTION 128**

A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

- A. A packet capture
- B. A user behavior analysis
- C. Threat hunting
- D. Credentialed vulnerability scanning

**Answer: C**

**NEW QUESTION 133**

Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

- A. The document is a honeypot and is meant to attract the attention of a cyberintruder.
- B. The document is a backup file if the system needs to be recovered.
- C. The document is a standard file that the OS needs to verify the login credentials.
- D. The document is a keylogger that stores all keystrokes should the account be compromised.

**Answer: A**

**NEW QUESTION 138**

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 142**

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 144**

A security assessment determines DES and 3DES at still being used on recently deployed production servers. Which of the following did the assessment identify?

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

**Answer: D**

**NEW QUESTION 148**

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. Order of volatility
- D. A log analysis
- E. A right-to-audit clause

**Answer: D**

**NEW QUESTION 150**

Ann, a forensic analyst, needs to prove that the data she originally acquired has remained unchanged while in her custody. Which of the following should Ann use?

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

**Answer:** A

**NEW QUESTION 153**

A security modern 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 m 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 analysts 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 154**

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. dnsenum
- D. logger

**Answer:** A

**NEW QUESTION 158**

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 159**

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 164**

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 168**

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 169

A nuclear plant was the victim of a recent attack, and all the networks were air gapped. A subsequent investigation revealed a worm as the source of the issue. Which of the following BEST explains what happened?

- A. A malicious USB was introduced by an unsuspecting employee.
- B. The ICS firmware was outdated
- C. A local machine has a RAT installed.
- D. The HVAC was connected to the maintenance vendor.

**Answer:** A

#### NEW QUESTION 170

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 173

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 177

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

- A. Asymmetric
- B. Symmetric
- C. Homeomorphic
- D. Ephemeral

**Answer:** B

#### NEW QUESTION 182

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 184

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 186

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 189

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 191

An.. 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 192

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 196

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 199

An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

- A. Reputation damage
- B. Identity theft
- C. Anonymization
- D. Interrupted supply chain

**Answer:** A

#### NEW QUESTION 203

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 208

Which of the following algorithms has the SMALLEST key size?

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

**Answer:** B

#### NEW QUESTION 212

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 213

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 214

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

- A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
- B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
- C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
- D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

**Answer:** D

#### NEW QUESTION 216

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 219

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:

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

- A. The end user purchased and installed a 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 224**

Which of the following would cause a Chief Information Security Officer (CISO) the MOST concern regarding newly installed Internet-accessible 4K surveillance cameras?

- A. An inability to monitor 100%, of every facility could expose the company to unnecessary risk.
- B. The cameras could be compromised if not patched in a timely manner.
- C. Physical security at the facility may not protect the cameras from theft.
- D. Exported videos may take up excessive space on the file servers.

**Answer:** A

**NEW QUESTION 229**

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 231**

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 233**

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 235**

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 237**

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 238**

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 243

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 246

A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.)

- A. Dual power supply
- B. Off-site backups
- C. Automatic OS upgrades
- D. NIC teaming
- E. Scheduled penetration testing
- F. Network-attached storage

**Answer:** AB

#### NEW QUESTION 247

Several large orders of merchandise were recently purchased on an e-commerce company's website. The totals for each of the transactions were negative values, resulting in credits on the customers' accounts. Which of the following should be implemented to prevent similar situations in the future?

- A. Ensure input validation is in place to prevent the use of invalid characters and values.
- B. Calculate all possible values to be added together and ensure the use of the proper integer in the code.
- C. Configure the web application firewall to look for and block session replay attacks.
- D. Make sure transactions that are submitted within very short time periods are prevented from being processed.

**Answer:** A

#### NEW QUESTION 252

After a phishing scam for a user's credentials, the red team was able to craft a payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session. Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

**Answer:** A

#### NEW QUESTION 255

A security analyst is hardening a Linux workstation and must ensure it has public keys forwarded to remote systems for secure login. Which of the following steps should the analyst perform to meet these requirements? (Select TWO).

- A. Forward the keys using ssh-copy-id.
- B. Forward the keys using scp.
- C. Forward the keys using ash -i.
- D. Forward the keys using openssl -s.
- E. Forward the keys using ssh-keygen.

**Answer:** AD

#### NEW QUESTION 258

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 260**

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 263**

A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

- A. One-time passwords
- B. Email tokens
- C. Push notifications
- D. Hardware authentication

**Answer:** C

**NEW QUESTION 264**

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

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 265**

Which of the following types of controls is a turnstile?

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

**Answer:** A

**NEW QUESTION 268**

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

- A. The system was configured with weak default security settings.
- B. The device uses weak encryption ciphers.
- C. The vendor has not supplied a patch for the appliance.
- D. The appliance requires administrative credentials for the assessment.

**Answer:** C

**NEW QUESTION 273**

A cybersecurity department purchased a new PAM solution. The team is planning to randomize the service account credentials of the Windows server first. Which of the following would be the BEST method to increase the security on the Linux server?

- A. Randomize the shared credentials
- B. Use only guest accounts to connect.
- C. Use SSH keys and remove generic passwords
- D. Remove all user accounts.

**Answer:** C

**NEW QUESTION 277**

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 281

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 284

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 289

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 get 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 292

Which of the following is the purpose of a risk register?

- A. To define the level of risk using probability and likelihood
- B. To register the risk with the required regulatory agencies
- C. To identify the risk, the risk owner, and the risk measures
- D. To formally log the type of risk mitigation strategy the organization is using

**Answer: C**

**NEW QUESTION 294**

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 299**

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

- A. A non-disclosure agreement
- B. Least privilege
- C. An acceptable use policy
- D. Ofboarding

**Answer:** D

**NEW QUESTION 303**

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 307**

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 308**

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 310**

A Chief Executive Officer's (CEO) personal information was stolen in a social engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

- A. Automated information sharing
- B. Open-source intelligence
- C. The dark web
- D. Vulnerability databases

**Answer:** C

**NEW QUESTION 311**

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 handle 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 316**

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 321**

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 326**

The Chief Security Officer (CSO) at a major hospital wants to implement SSO to help improve in the environment patient data, particularly at shared terminals. The Chief Risk Officer (CRO) is concerned that training and guidance have been provided to frontline staff, and a risk analysis has not been performed. Which of the following is the MOST likely cause of the CRO's concerns?

- A. SSO would simplify username and password management, making it easier for hackers to pass guess accounts.
- B. SSO would reduce password fatigue, but staff would still need to remember more complex passwords.
- C. SSO would reduce the password complexity for frontline staff.
- D. SSO would reduce the resilience and availability of system if the provider goes offline.

**Answer:** D

**NEW QUESTION 328**

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 329**

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 331**

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. Eradication
- D. Recovery
- E. Containment

**Answer:** E

**NEW QUESTION 336**

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 337**

A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

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

**Answer:** D

**NEW QUESTION 339**

A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

Which of the following will the forensics investigator MOST likely determine has occurred?

- A. SQL injection
- B. CSRF
- C. XSS
- D. XSRF

**Answer:** B

**NEW QUESTION 340**

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 344**

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

Perform the following steps:

- \* 1. Configure the RADIUS server.
- \* 2. Configure the WiFi controller.
- \* 3. Preconfigure the client for an incoming guest.

The guest AD credentials are: User: guest01

Password: guestpass



B. Not Mastered

**Answer:** A

**Explanation:**

Use the same settings as describe in below images.

Graphical user interface, application Description automatically generated

Graphical user interface, text, application, chat or text message Description automatically generated

**NEW QUESTION 346**

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 350**

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 351**

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 356**

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 359

The SOC is reviewing process and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. The allowed the malware to spread to additional hosts before it was contained. Which of the following would be BEST to improve the incident response process?

- A. Updating the playbooks with better decision points
- B. Dividing the network into trusted and untrusted zones
- C. Providing additional end-user training on acceptable use
- D. Implementing manual quarantining of infected hosts

**Answer:** A

#### NEW QUESTION 361

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 363

A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

- A. A RAT
- B. Ransomware
- C. Polymorphic
- D. A worm

**Answer:** C

#### NEW QUESTION 367

A network administrator would like to configure a site-to-site VPN utilizing IPSec. The administrator wants the tunnel to be established with data integrity encryption, authentication and anti- replay functions Which of the following should the administrator use when configuring the VPN?

- A. AH
- B. EDR
- C. ESP
- D. DNSSEC

**Answer:** C

#### NEW QUESTION 371

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 374

A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers Which of the following tools should the analyst use?

- A. netstat
- B. net share
- C. netcat
- D. nbtstat
- E. net session

**Answer:** A

**NEW QUESTION 379**

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 380**

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

Which of the following BEST describes this kind of attack?

- A. Directory traversal
- B. SQL injection
- C. API
- D. Request forgery

**Answer:** D

**NEW QUESTION 385**

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 386**

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 389**

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 390**

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 395**

A malicious actor recently penetrated 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 396**

The lessons-learned analysis from a recent incident reveals that an administrative office worker received a call from someone claiming to be from technical support. The caller convinced the office worker to visit a website, and then download and install a program masquerading as an antivirus package. The program was actually a backdoor that an attacker could later use to remote control the worker's PC. Which of the following would be BEST to help prevent this type of attack in the future?

- A. Data loss prevention
- B. Segmentation
- C. Application whitelisting
- D. Quarantine

**Answer:** C

**NEW QUESTION 398**

A worldwide manufacturing company has been experiencing email account compromise. 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 400**

A SOC 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. ADMZ
- C. DLP
- D. File integrity monitoring

**Answer:** A

**NEW QUESTION 403**

Which of the following is a team of people dedicated to 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 406**

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 as 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 411

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 412

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 414

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list
- D. A complex password policy

**Answer:** B

#### NEW QUESTION 415

An organization blocks user access to command-line interpreters but hackers still managed to invoke the interpreters using native administrative tools Which of the following should the security team do to prevent this from happening in the future?

- A. Implement HIPS to block inbound and outbound SMB ports 139 and 445.
- B. Trigger a SIEM alert whenever the native OS tools are executed by the user
- C. Disable the built-in OS utilities as long as they are not needed for functionality.
- D. Configure the AV to quarantine the native OS tools whenever they are executed

**Answer:** C

#### NEW QUESTION 416

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

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 420

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 -sV
- D. nslookup -port=80 comptia.org

**Answer:** C

**NEW QUESTION 423**

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 425**

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 426**

An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

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

**Answer:** A

**NEW QUESTION 428**

Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

- A. Whaling
- B. Spam
- C. Invoice scam
- D. Pharming

**Answer:** A

**NEW QUESTION 431**

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 436**

The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

- A. Install a NIDS device at the boundary.
- B. Segment the network with firewalls.
- C. Update all antivirus signatures daily.
- D. Implement application blacklisting.

**Answer:** B

**NEW QUESTION 440**

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 441

A user recent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

**Answer:** D

#### NEW QUESTION 442

The new Chief Executive Officer (CEO) of a large company has announced a partnership with a vendor that will provide multiple collaboration applications t 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 445

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 447

A user contacts the help desk to report the following:

Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.

The user was able to access the Internet but had trouble accessing the department share until the next day.

The user is now getting notifications from the bank about unauthorized transactions. Which of the following attack vectors was MOST likely used in this scenario?

- A. Rogue access point
- B. Evil twin
- C. DNS poisoning
- D. ARP poisoning

**Answer:** A

#### NEW QUESTION 451

A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

- A. Repository transaction logs
- B. Common Vulnerabilities and Exposures
- C. Static code analysis
- D. Non-credentialed scans

**Answer:** C

#### NEW QUESTION 456

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 461



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 464**

A forensics examiner is attempting to dump password cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

- A. The examiner does not have administrative privileges to the system
- B. The system must be taken offline before a snapshot can be created
- C. Checksum mismatches are invalidating the disk image
- D. The swap file needs to be unlocked before it can be accessed

**Answer:** D

#### **NEW QUESTION 469**

The following are the logs of a successful attack.

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 474**

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 477**

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 481**

.....



## 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](#)**