CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1
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 2
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 3
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

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

Which of the following solutions would meet the requirements?

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

Answer: D

NEW QUESTION 4
Which of the following describes the BEST approach for deploying application patches?

A. Apply the patches to systems in a testing environment then to systems in a staging environment, and finally to production systems.
B. Test the patches in a staging environment, develop against them in the development environment, andthen apply them to the production systems
C. Test the patches m a test environment apply them to the production systems and then apply them to a staging environment
D. Apply the patches to the production systems apply them in a staging environment, and then test all of them in a testing environment

Answer: A

NEW QUESTION 5
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. Unsecme protocols
B. Default settings
C. Open permissions
D. Weak encryption

Answer: D

NEW QUESTION 6
A security engineer needs to enhance MFA access to sensitive areas in a building. A key card and fingerprint scan are already in use. Which of the following would add another factor of authentication?

A. Hard token
B. Retina scan
C. SMS text
D. Keypad PIN

Answer: B

NEW QUESTION 7
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 8
A security analyst is reviewing the following attack log output:

```
user comptia\john.smith attempted login with the password password123
user comptia\jane.doe attempted login with the password password123
user comptia\user.one attempted login with the password password123
user comptia\user.two attempted login with the password password123
user comptia\user.three attempted login with the password password123

user comptia\john.smith attempted login with the password password234
user comptia\jane.doe attempted login with the password password234
user comptia\user.one attempted login with the password password234
user comptia\user.two attempted login with the password password234
user comptia\user.three attempted login with the password password234
```

Which of the following types of attacks does this MOST likely represent?

A. Rainbow table
B. Brute-force
C. Password-spraying
D. Dictionary

Answer: C

NEW QUESTION 9
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 10
After a ransomware attack a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. Which of the following will the company MOST likely review to trace this transaction?

A. The public ledger
B. The NetFlow data
C. A checksum
D. The event log

Answer: A

NEW QUESTION 10
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 14
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 15
A security engineer is reviewing log files after a third discovered usernames and passwords for the organization's accounts. The engineer sees there was a change in the IP address for a vendor website one earlier. This change lasted eight hours. Which of the following attacks was MOST likely used?

A. Man-in- the middle
B. Spear-phishing
C. Evil twin
D. DNS poising

Answer: D

NEW QUESTION 19
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 20
A system administrator needs to implement an access control scheme that will allow an object's access policy be determined by its owner. Which of the following access control schemes BEST fits the requirements?

A. Role-based access control
B. Discretionary access control
C. Mandatory access control
D. Attribute-based access control

Answer: B

NEW QUESTION 23
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 26
To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS
B. laaS
C. SaaS
D. PaaS

Answer: D

NEW QUESTION 31
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 33
A workwide 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 36
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 41
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 44
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 49
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 52
A security engineer needs to Implement the following requirements:
• All Layer 2 switches should leverage Active Directory tor 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 56
A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who has local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.
B. Segment the network into trusted and untrusted zones.
C. Enforce application whitelisting.
D. Implement DLP at the network boundary.

Answer: C

NEW QUESTION 58
A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:

- www.company.com (main website)
- contactus.company.com (for locating a nearby location)
- quotes.company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

A. SAN
B. Wildcard
C. Extended validation
D. Self-signed

Answer: B

NEW QUESTION 59
Which of the following would be BEST to establish between organizations to define the responsibilities of each party outline the key deliverables and include monetary penalties for breaches to manage third-party risk?

A. An ARO
B. An MOU
C. An SLA
D. A BPA

Answer: B

NEW QUESTION 61
Which of the following algorithms has the SMALLEST key size?

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

Answer: B

NEW QUESTION 65
An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

Answer: BD

NEW QUESTION 70
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 73
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 74
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 79
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 83
Which of the following would MOST likely support the integrity of a voting machine?

A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

Answer: D

NEW QUESTION 88
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 89
During an incident response, a security analyst observes the following log entry on the web server.

```
GET http://www.companysite.com/product_info.php?show=../../../../etc/passwd HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experience?

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

Answer: B

NEW QUESTION 90
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 91
A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

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

Answer: C

NEW QUESTION 93
Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

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

Answer: A

NEW QUESTION 97
A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two- drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

A. 1
B. 5
C. 6

Answer: B

NEW QUESTION 102
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: D

NEW QUESTION 104
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 107
Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hot-spots?

A. Footprinting
B. White-box testing
C. A drone/UAV
D. Pivoting

Answer: A

NEW QUESTION 108
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 113
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 116
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 121
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 126
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 129
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 131
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 135
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 138
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 143
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 144
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 145
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 147
Which of the following types of controls is a turnstile?

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

Answer: A

NEW QUESTION 151
A company has determined that if its computer-based manufacturing is not functioning for 12 consecutive hours, it will lose more money that it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

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

Answer: C

NEW QUESTION 156
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/MME 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 161
An organization hired a consultant to assist with an active attack, and the consultant was able to identify the compromised accounts and computers. Which of the following is the consultant MOST likely to recommend to prepare for eradication?

A. Quarantining the compromised accounts and computers, only providing them with network access
B. Segmenting the compromised accounts and computers into a honeynet so as to not alert the attackers.
C. Isolating the compromised accounts and computers, cutting off all network and internet access.
D. Logging off and deleting the compromised accounts and computers to eliminate attacker access.

Answer: B

NEW QUESTION 162
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 DIP 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 165
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 170
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 174
A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plan 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 177
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: A

NEW QUESTION 181
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 186
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 187
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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