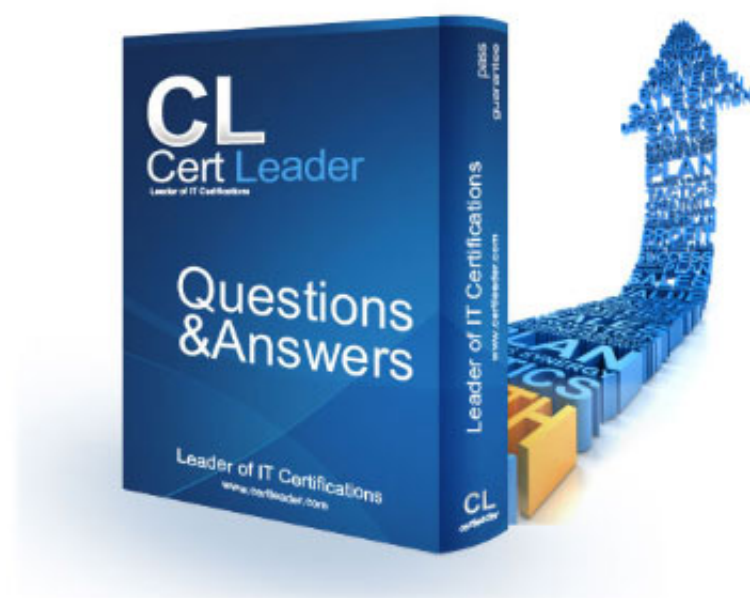


SY0-601 Dumps

CompTIA Security+ Exam

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



NEW QUESTION 1

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 2

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

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

Answer: B

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 9

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

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 10

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 11

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 16

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

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

Answer: C

NEW QUESTION 21

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

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

Answer: D

NEW QUESTION 24

The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

- A. install a smart meter on the staff WiFi.
- B. Place the environmental systems in the same DHCP scope as the staff WiFi.
- C. Implement Zigbee on the staff WiFi access points.
- D. Segment the staff WiFi network from the environmental systems network.

Answer: D

NEW QUESTION 27

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

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

Answer: D

NEW QUESTION 29

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 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 32

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

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

Answer: AB

NEW QUESTION 37

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

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

Answer:

D

NEW QUESTION 41

A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

- A. The scan results show open ports, protocols, and services exposed on the target host
- B. The scan enumerated software versions of installed programs
- C. The scan produced a list of vulnerabilities on the target host
- D. The scan identified expired SSL certificates

Answer: B

NEW QUESTION 42

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 44

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 46

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 47

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

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

Answer: A

NEW QUESTION 50

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 51

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

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

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

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

Answer: C

NEW QUESTION 52

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

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

Answer: C

NEW QUESTION 55

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 57

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

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

Answer: D

NEW QUESTION 58

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 59

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

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

Answer: C

NEW QUESTION 61

A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

- A. Loss of proprietary information
- B. Damage to the company's reputation
- C. Social engineering
- D. Credential exposure

Answer: C

NEW QUESTION 65

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

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

Answer: B

NEW QUESTION 66

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

- A. Nmap
- B. Wireshark
- C. Autopsy
- D. DNSEnum

Answer: A

NEW QUESTION 70

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 73

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

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:ab0f:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

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

Answer: A

NEW QUESTION 75

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 80

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 81

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 84

Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

- A. Investigation
- B. Containment
- C. Recovery
- D. Lessons learned

Answer: B

NEW QUESTION 86

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 89

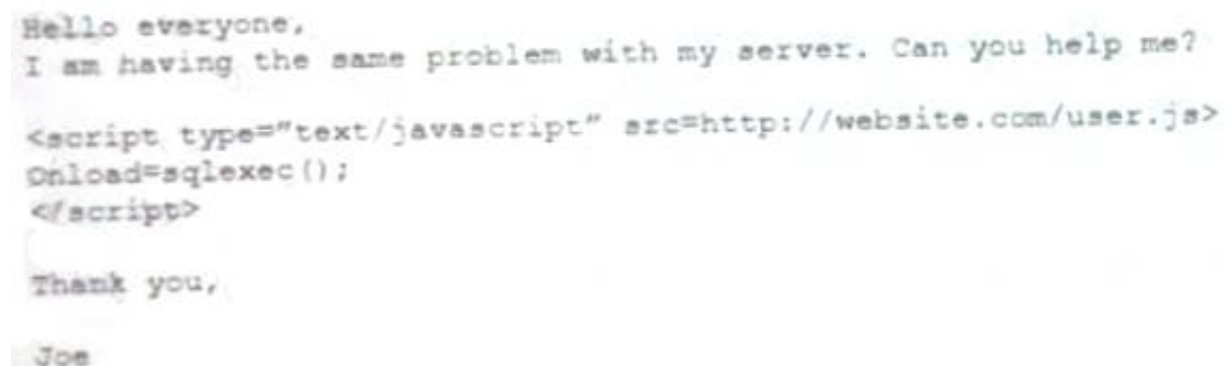
A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

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

Answer: D

NEW QUESTION 90

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



Hello everyone,
I am having the same problem with my server. Can you help me?

```
<script type="text/javascript" src=http://website.com/user.js>  
Onload=sqlexec();  
</script>
```

Thank you,

Joe

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

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

Answer: C

NEW QUESTION 93

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 96

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 98

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

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

Answer: D

NEW QUESTION 100

In which of the following risk management strategies would cybersecurity insurance be used?

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

Answer: A

NEW QUESTION 105

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

- A. RAID 0
- B. RAID 1
- C. RAID 5
- D. RAID 10

Answer: C

NEW QUESTION 106

Which of the following types of controls is a turnstile?

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

Answer: A

NEW QUESTION 111

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 113

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

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

Answer: B

NEW QUESTION 114

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

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

Answer: A

NEW QUESTION 118

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

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

Answer: D

NEW QUESTION 123

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

- Mobile device OSs must be patched up to the latest release
- A screen lock must be enabled (passcode or biometric)
- Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

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

Answer: DE

NEW QUESTION 124

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

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

Answer: A

NEW QUESTION 125

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 126

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

prevent the exfiltration of data? (Select TWO).

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

Answer: BE

NEW QUESTION 127

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 131

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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