

# Exam Questions SY0-601

CompTIA Security+ Exam

<https://www.2passeasy.com/dumps/SY0-601/>



#### NEW QUESTION 1

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 2

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 3

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 4

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

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

**Answer:** C

#### NEW QUESTION 5

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 6

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 7

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 8

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 9

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 10

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 10

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

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

**Answer:** A

#### NEW QUESTION 12

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

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- F. Outdated anti-malware software

**Answer:** AD

#### NEW QUESTION 14

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

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

**Answer:** D

#### NEW QUESTION 16

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

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

**Answer:** C

#### NEW QUESTION 21

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 26

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 31

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 33

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 37

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 40

A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

- A. DAC
- B. ABAC
- C. SCAP
- D. SOAR

**Answer:** D

#### NEW QUESTION 45

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

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

**Answer:** A

#### NEW QUESTION 47

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. tail
- E. curl
- F. openssl
- G. dd

**Answer:** AB

#### NEW QUESTION 51

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 53

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 poisoning

**Answer:** D

#### NEW QUESTION 57



A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:

```
3/16/20 3:31:10 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:11 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:12 AM Audit Failure: CompanyNetwork\User1 Unknown username or bad password.
3/16/20 3:31:13 AM Audit Failure: CompanyNetwork\User1 Account locked out.
3/16/20 3:31:14 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:15 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:16 AM Audit Failure: CompanyNetwork\User2 Unknown username or bad password.
3/16/20 3:31:18 AM Audit Failure: CompanyNetwork\User2 Account locked out.
3/16/20 3:31:19 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:20 AM Audit Failure: CompanyNetwork\User3 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Success: CompanyNetwork\User3 Successful logon.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:31:22 AM Audit Failure: CompanyNetwork\User4 Unknown username or bad password.
3/16/20 3:32:40 AM Audit Failure: CompanyNetwork\User4 Successful logon.
3/16/20 3:33:25 AM Audit Success: CompanyNetwork\User4 Successful logon.
```

Which of the following attacks MOST likely occurred?

- A. Dictionary
- B. Credential-stuffing
- C. Password-spraying
- D. Brute-force

**Answer:** D

#### NEW QUESTION 62

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 66

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 following 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 68

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

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

**Answer:** C

#### NEW QUESTION 71

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 75

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

protect the environment from this malware?

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

**Answer:** C

#### NEW QUESTION 79

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 81

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 85

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 88

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 93

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

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

**Answer:** B

#### NEW QUESTION 97

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 98

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 99

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 102

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 106

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

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

**Answer:** C

#### NEW QUESTION 108

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 111

A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this task?

- A. Netcat
- B. Netstat
- C. Nmap
- D. Nessus

**Answer:** B

#### NEW QUESTION 114

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



Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

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

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

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

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

**Answer: D**

#### NEW QUESTION 119

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 123

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

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

**Answer: D**

#### NEW QUESTION 127

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 132

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 134

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

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

**Answer: C**

#### NEW QUESTION 138

A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?

- A. Segmentation
- B. Containment
- C. Geofencing
- D. Isolation

**Answer: A**

#### NEW QUESTION 142

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

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

**Answer: D**

#### NEW QUESTION 144

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 149

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 152

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

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

**Answer: B**

#### NEW QUESTION 157

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 160

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

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

Which of the following is the security analyst observing?

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

**Answer: C**

#### NEW QUESTION 161

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 166

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 171

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 175

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 178

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

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

**Answer:** C

#### NEW QUESTION 183

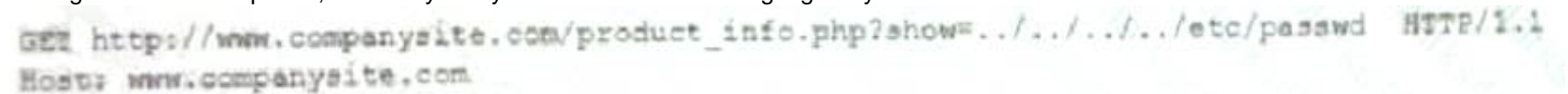
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the Internet all day. Which of the following would MOST likely show where the malware originated?

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

**Answer:** A

#### NEW QUESTION 184

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 experiencing?

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

**Answer:** B

#### NEW QUESTION 188

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 189

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 191

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:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```

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 194

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



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

**Answer:** C

#### NEW QUESTION 197

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 202

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 206

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 207

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

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

**Answer:** C

#### NEW QUESTION 208

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 212

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 216



A company is launching a new internet platform for its clients. The company does not want to implement its own authorization solution but instead wants to rely on the authorization provided by another platform. Which of the following is the BEST approach to implement the desired solution?

- A. OAuth
- B. TACACS+
- C. SAML
- D. RADIUS

**Answer:** D

#### NEW QUESTION 218

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

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

**Answer:** E

#### NEW QUESTION 219

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

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

**Answer:** A

#### NEW QUESTION 222

A security analyst is investigating an incident that was first reported as an issue connecting to network shares and the internet. While reviewing logs and tool output, the analyst sees the following:

IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

- A. IP conflict
- B. Pass-the-hash
- C. MAC flooding
- D. Directory traversal
- E. ARP poisoning

**Answer:** E

#### NEW QUESTION 225

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

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

**Answer:** BD

#### NEW QUESTION 229

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 234

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

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

**Answer:** A

#### NEW QUESTION 239

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

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

**Answer:** C

#### NEW QUESTION 243

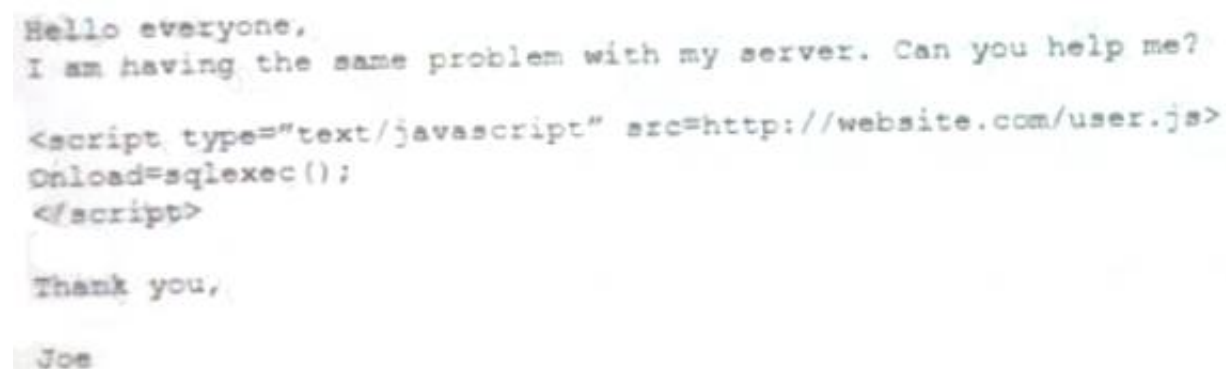
A manufacturer creates designs for very high security products that are required to be protected and controlled by the government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

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

**Answer:** A

#### NEW QUESTION 248

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 251

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 255

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 258

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 261

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 265

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 266

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

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

**Answer:** A

#### NEW QUESTION 270

A security administrator needs to create a RAID 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 275

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

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

**Answer:** C

#### NEW QUESTION 279

Which of the following types of controls is a turnstile?

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

**Answer:** A

#### NEW QUESTION 280

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 282

An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

- A. Incident response
- B. Communications
- C. Disaster recovery
- D. Data retention

**Answer:** C

#### NEW QUESTION 287

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 291

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 294

A forensics investigator is examining a number of unauthorized payments the 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 298

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 301

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 304

A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

- A. Nmapn
- B. Heat maps
- C. Network diagrams
- D. Wireshark

**Answer:** C

#### NEW QUESTION 306

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 308

A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

- A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
- B. Restrict administrative privileges and patch ail systems and applications.
- C. Rebuild all workstations and install new antivirus software
- D. Implement application whitelisting and perform user application hardening

**Answer:** A

#### NEW QUESTION 313

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 316

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 320

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 323**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-601 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-601 Product From:

<https://www.2passeasy.com/dumps/SY0-601/>

## Money Back Guarantee

### **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