

# Exam Questions SY0-601

CompTIA Security+ Exam

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



#### NEW QUESTION 1

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, incident during a pandemic or crisis, However, the CEO is concerned that some staff members may take advantage of the of the flexibility and work from high-risk countries while on holidays work to a third-party organization in another country. The Chief information Officer (CIO) believes the company can implement some basic to mitigate the majority of the risk. Which of the following would be BEST to mitigate CEO's concern? (Select TWO).

- A. Geolocation
- B. Time-of-day restrictions
- C. Certificates
- D. Tokens
- E. Geotagging
- F. Role-based access controls

**Answer:** AE

#### NEW QUESTION 2

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 continues to evade detection. Which of the following should 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 3

A database administrator needs to ensure all passwords are stored in a secure manner, so the administrate 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 4

An attacker is attempting to exploit users by creating a fake website with the URL users. Which of the following social-engineering attacks does this describe?

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

**Answer:** D

#### NEW QUESTION 5

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

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

**Answer:** D

#### NEW QUESTION 6

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 7

A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively.
- Occasional personal use is acceptable due to the travel requirements.
- Users must be able to install and configure sanctioned programs and productivity suites.
- The devices must be encrypted
- The devices must be capable of operating in low-bandwidth environments.

Which of the following would provide the GREATEST benefit to the security posture of the devices?

- A. Configuring an always-on VPN
- B. Implementing application whitelisting
- C. Requiring web traffic to pass through the on-premises content filter
- D. Setting the antivirus DAT update schedule to weekly

**Answer:** A

#### NEW QUESTION 8

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 9

An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

- A. Require a complex, eight-character password that is updated every 90 days.
- B. Perform only non-intrusive scans of workstations.
- C. Use non-credentialed scans against high-risk servers.
- D. Log and alert on unusual scanner account logon times.

**Answer:** D

#### NEW QUESTION 10

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

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

**Answer:** C

#### NEW QUESTION 10

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

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

**Answer:** C

#### NEW QUESTION 12

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

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

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

**Answer:** B

#### NEW QUESTION 15

A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

- A. NIC teaming
- B. High availability
- C. Dual power supply
- D. IaaS

**Answer:** B

**NEW QUESTION 17**

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 20**

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 21**

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

**INSTRUCTIONS**

Click on each firewall to do the following:

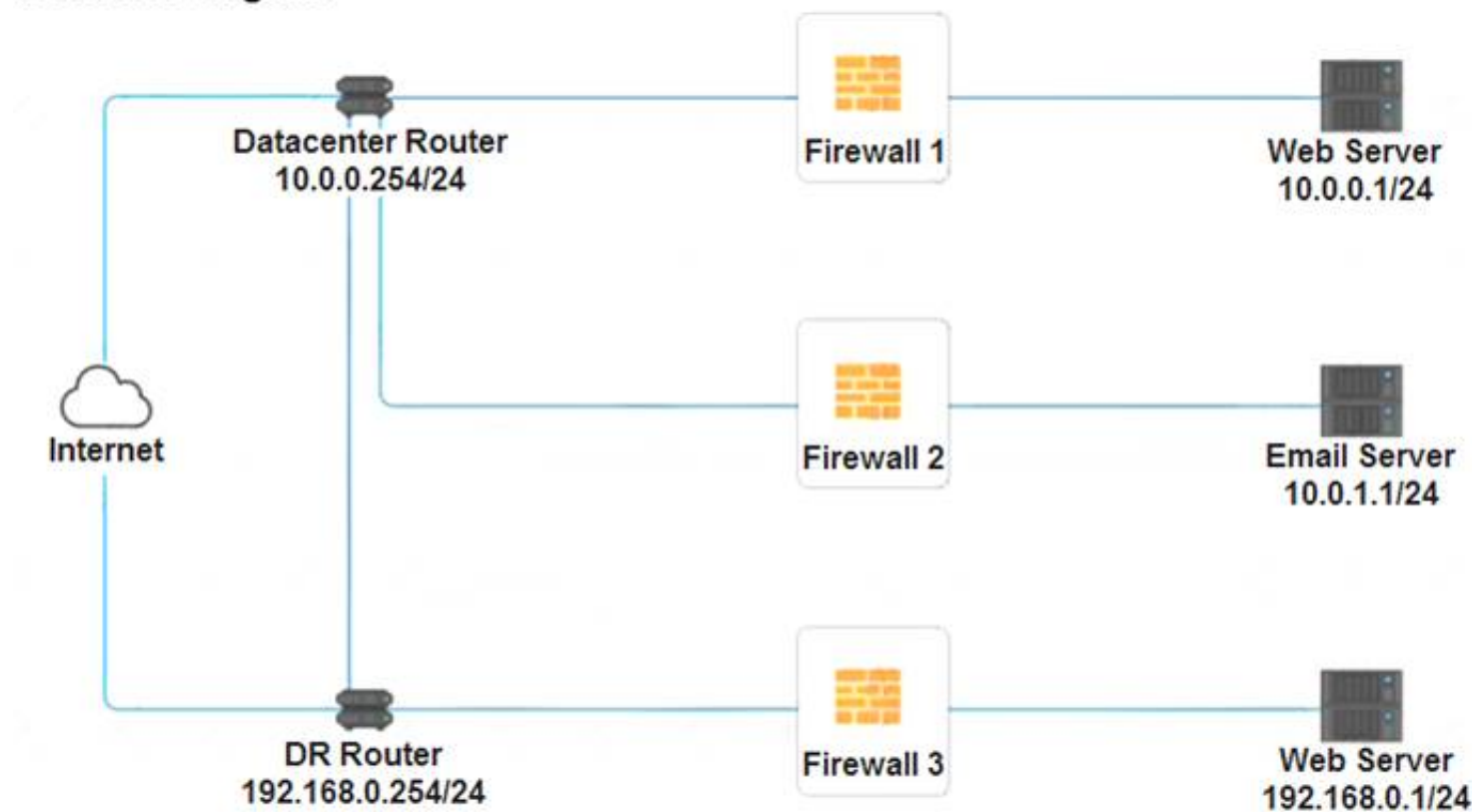
Deny cleartext web traffic.

Ensure secure management protocols are used.

Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

**Network Diagram**

Firewall 1

Rule Name	Source	Destination	Service	Action
DNS Rule	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
HTTPS Outbound	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
Management	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
HTTPS Inbound	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>
HTTP Inbound	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  10.0.0.1/24  10.0.1.1/24  192.168.0.1/24 </div>	<div> <div></div> <div>▼</div> </div> <div> ANY  DNS  HTTP  HTTPS  TELNET  SSH </div>	<div> <div></div> <div>▼</div> </div> <div> PERMIT  DENY </div>

Reset Answer
Save
Close



**Firewall 3**
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           PERMIT            DENY         </div> </div>
HTTPS Outbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           PERMIT            DENY         </div> </div>
Management	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           PERMIT            DENY         </div> </div>
HTTPS Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           PERMIT            DENY         </div> </div>
HTTP Inbound	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            10.0.0.1/24            10.0.1.1/24            192.168.0.1/24         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           ANY            DNS            HTTP            HTTPS            TELNET            SSH         </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span></span> <span>▼</span> </div> <div>           PERMIT            DENY         </div> </div>

Reset Answer
Save
Close

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Firewall 1:

**Firewall 1**
✕

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY

Reset Answer
Save
Close

Firewall 1					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.0.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.0.1/24	• SSH	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.0.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.0.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

Firewall 2:

Firewall 2					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.1.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.1.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.1.1/24	• DNS	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.1.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.1.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

Firewall 2					
Rule Name	Source	Destination	Service	Action	
DNS Rule	10.0.1.1/24	• ANY	• DNS	• PERMIT	•
HTTPS Outbound	10.0.1.1/24	• ANY	• HTTPS	• PERMIT	•
Management	ANY	• 10.0.1.1/24	• DNS	• PERMIT	•
HTTPS Inbound	ANY	• 10.0.1.1/24	• HTTPS	• PERMIT	•
HTTP Inbound	ANY	• 10.0.1.1/24	• HTTP	• DENY	•
<div>Reset Answer</div> <div>Save</div> <div>Close</div>					

Firewall 3:

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	• DENY

Firewall 3				
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	• ANY	• DNS	• PERMIT
HTTPS Outbound	192.168.0.1/24	• ANY	• HTTPS	• PERMIT
Management	ANY	• 192.168.0.1/24	• SSH	• PERMIT
HTTPS Inbound	ANY	• 192.168.0.1/24	• HTTPS	• PERMIT
HTTP Inbound	ANY	• 192.168.0.1/24	• HTTP	DENY

DNS Rule – ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound – 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT Management – ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound – ANY --> ANY --> HTTPS --> PERMIT HTTP Inbound – ANY --> ANY --> HTTP --> DENY

#### NEW QUESTION 25

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

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

Answer: D

#### NEW QUESTION 30

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

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

Answer: D

#### NEW QUESTION 33

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 35

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 38

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

- A. RA
- B. OCSP
- C. CRL
- D. CSR

**Answer:** C

#### NEW QUESTION 40

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 41

A recent malware outbreak across a subnet included successful rootkit installations on many PCs, ensuring persistence by rendering remediation efforts ineffective. Which of the following would BEST detect the presence of a rootkit in the future?

- A. FDE
- B. NIDS
- C. EDR
- D. DLP

**Answer:** C

#### NEW QUESTION 46

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 48

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 50

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 51

An organization relies on third-party video conferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality video conferencing while minimizing latency when connected to the VPN?

- A. Using geographic diversity to have VPN terminators closer to end users
- B. Utilizing split tunneling so only traffic for corporate resources is encrypted
- C. Purchasing higher-bandwidth connections to meet the increased demand
- D. Configuring QoS properly on the VPN accelerators

**Answer:** D

#### NEW QUESTION 55

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

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

**Answer:** BD

#### NEW QUESTION 56

Which of the following is a reason why an organization would define an AUP?

- A. To define the lowest level of privileges needed for access and use of the organization's resources
- B. To define the set of rules and behaviors for users of the organization's IT systems
- C. To define the intended partnership between two organizations
- D. To define the availability and reliability characteristics between an IT provider and consumer

**Answer:** B

#### NEW QUESTION 58

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 59

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

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

**Answer:** A

#### NEW QUESTION 64

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 65

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:

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 66

An organization is having difficulty correlating events from its individual AV. EDR. DLP. SWG. WAF. MOM. HIPS, and CASB systems. Which of the following is the BEST way to improve the situation?

- A. Remove expensive systems that generate few alerts.
- B. Modify the systems to alert only on critical issues.
- C. Utilize a SIEM to centralize logs and dashboards.
- D. Implement a new syslog/NetFlow appliance.

**Answer: C**

#### NEW QUESTION 68

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 all 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 73

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 77

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

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

**Answer: B**

#### NEW QUESTION 81

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned that servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

- A. 135
- B. 139
- C. 143
- D. 161
- E. 443
- F. 445

**Answer:** AE

#### NEW QUESTION 83

Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

- A. DNSSEC and DMARC
- B. DNS query logging
- C. Exact mail exchanger records in the DNS
- D. The addition of DNS conditional forwarders

**Answer:** C

#### NEW QUESTION 86

An.. that has a large number of mobile devices is exploring enhanced security controls to manage unauthorized access if a device is lost or stolen. Specifically, if mobile devices are more than 3mi (4 8km) from the building, the management team would like to have the security team alerted and server resources restricted on those devices. Which of the following controls should the organization implement?

- A. Geofencing
- B. Lockout
- C. Near-field communication
- D. GPS tagging

**Answer:** A

#### NEW QUESTION 88

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 92

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 95

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

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

**Answer:** A

#### NEW QUESTION 100

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 105

An attacker is attempting to exploit users by creating a fake website with the URL [www.validwebsite.com](http://www.validwebsite.com). The attacker's intent is to imitate the look and feel of a



legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

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

**Answer:** D

#### NEW QUESTION 106

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

- A. Unsecured root accounts
- B. Zero day
- C. Shared tenancy
- D. Insider threat

**Answer:** C

#### NEW QUESTION 107

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

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

**Answer:** B

#### NEW QUESTION 110

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 114

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 116

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

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

**Answer:** A

#### NEW QUESTION 117

Which of the following represents a biometric FRR?

- A. Authorized users being denied access
- B. Users failing to enter the correct PIN
- C. The denied and authorized numbers being equal
- D. The number of unauthorized users being granted access

**Answer:** A

#### NEW QUESTION 119

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The Oss

are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

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

**Answer:** D

#### NEW QUESTION 121

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key
- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

**Answer:** BC

#### NEW QUESTION 122

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 125

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

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

**Answer:** B

#### NEW QUESTION 130

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:  
Which of the following attacks does the analyst MOST likely see in this packet capture?

- A. Session replay
- B. Evil twin
- C. Bluejacking
- D. ARP poisoning

**Answer:** B

#### NEW QUESTION 132

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

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

**Answer:** C

#### NEW QUESTION 136

An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

- A. Hping3 -s comptia.org -p 80
- B. Nc -1 -v comptia.org -p 80
- C. nmap comptia.org -p 80 -aV
- D. nslookup -port=80 comptia.org

**Answer:** C

#### NEW QUESTION 139

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 140

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 144

An analyst has determined that a server was not patched and an external actor exfiltrated data on port 139. Which of the following sources should the analyst review to BEST ascertain how the Incident could have been prevented?

- A. The vulnerability scan output
- B. The security logs
- C. The baseline report
- D. The correlation of events

**Answer: A**

#### NEW QUESTION 149

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

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

**Answer: BD**

#### NEW QUESTION 150

A security analyst is investigation 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 153

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

- A. Risk matrix
- B. Risk tolerance
- C. Risk register

D. Risk appetite

**Answer:** B

#### NEW QUESTION 156

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. When of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. VLAN
- D. A screened subnet

**Answer:** D

#### NEW QUESTION 158

Users at organization have been installing programs from the internet on their workstations without first proper authorization. The organization maintains a portal from which users can install standardized programs. However, some users have administrative access on their workstations to enable legacy programs to function properly. Which of the following should the security administrator consider implementing to address this issue?

- A. Application code signing
- B. Application whitelisting
- C. Data loss prevention
- D. Web application firewalls

**Answer:** B

#### NEW QUESTION 161

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 165

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:

- \* Employees must provide an alternate work location (i.e., a home address)
- \* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.

Which of the following BEST describes the MDM options the company is using?

- A. Geofencing, content management, remote wipe, containerization, and storage segmentation
- B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
- C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
- D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption

**Answer:** D

#### NEW QUESTION 169

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 171

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 173

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



to use in a threat mode?

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

**Answer:** A

#### NEW QUESTION 177

A company is designing the layout of a new datacenter so it will have an optimal environmental temperature Which of the following must be included? (Select TWO)

- A. An air gap
- B. A cold aisle
- C. Removable doors
- D. A hot aisle
- E. An IoT thermostat
- F. A humidity monitor

**Answer:** EF

#### NEW QUESTION 181

n organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

- A. The baseline
- B. The endpoint configurations
- C. The adversary behavior profiles
- D. The IPS signatures

**Answer:** C

#### NEW QUESTION 183

A security administrator is analyzing the corporate wireless network The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports Which erf the following attacks in happening on the corporate network?

- A. Man in the middle
- B. Evil twin
- C. Jamming
- D. Rogue access point
- E. Disassociation

**Answer:** B

#### NEW QUESTION 184

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

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

**Answer:** B

#### NEW QUESTION 186

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

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

**Answer:** C

#### NEW QUESTION 189

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

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

**Answer:** D

#### NEW QUESTION 190

Entering a secure area requires passing through two doors, both of which require someone who is already inside to initiate access. Which of the following types of physical security controls does this describe?

- A. Cameras
- B. Faraday cage
- C. Access control vestibule
- D. Sensors
- E. Guards

**Answer:** C

#### NEW QUESTION 193

An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

- A. Laptops
- B. Containers
- C. Thin clients
- D. Workstations

**Answer:** C

#### NEW QUESTION 196

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 199

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 201

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

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

**Answer:** B

#### NEW QUESTION 203

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

- A. Fileless malware
- B. A downgrade attack
- C. A supply-chain attack
- D. A logic bomb
- E. Misconfigured BIOS

**Answer:** C

#### NEW QUESTION 205

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

- A. Configure the perimeter firewall to deny inbound external connections to SMB ports.
- B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.
- C. Deny unauthenticated users access to shared network folders.
- D. Verify computers are set to install monthly operating system, updates automatically.

**Answer:** A

#### NEW QUESTION 206

A critical file server is being upgraded and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirements?

- A. RAID 0+1
- B. RAID 2
- C. RAID 5
- D. RAID 6

**Answer:** C

#### NEW QUESTION 210

A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident. During which of the following phases of the response process is this activity MOST likely occurring?

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

**Answer:** D

#### NEW QUESTION 213

.....

## 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