



SY0-301^{Q&As}

Security+ Certification Exam 2011 version

Pass CompTIA SY0-301 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/SY0-301.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

- A. Acceptable Use Policy
- B. Privacy Policy
- C. Security Policy
- D. Human Resource Policy

Correct Answer: A

QUESTION 2

Which of the following is the MOST important step for preserving evidence during forensic procedures?

- A. Involve law enforcement
- B. Chain of custody
- C. Record the time of the incident
- D. Report within one hour of discovery

Correct Answer: B

QUESTION 3

Used in conjunction, which of the following are PII? (Select TWO).

- A. Marital status
- B. Favorite movie
- C. Pet's name
- D. Birthday
- E. Full name

Correct Answer: DE

QUESTION 4

Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this



action remediate?

- A. Shoulder Surfing
- B. Dumpster Diving
- C. Phishing
- D. Impersonation

Correct Answer: B

QUESTION 5

Which of the following is described as an attack against an application using a malicious file?

- A. Client side attack
- B. Spam
- C. Impersonation attack
- D. Phishing attack

Correct Answer: A

QUESTION 6

Matt, an administrator, is concerned about the wireless network being discovered by war driving. Which of the following can be done to mitigate this?

- A. Enforce a policy for all users to authentic through a biometric device.
- B. Disable all SSID broadcasting.
- C. Ensure all access points are running the latest firmware.
- D. Move all access points into public access areas.

Correct Answer: B

QUESTION 7

Which of the following provides data the best fault tolerance at the LOWEST cost?

- A. Load balancing
- B. Clustering
- C. Server virtualization



D. RAID 6

Correct Answer: D

QUESTION 8

The Chief Information Security Officer (CISO) has mandated that all IT systems with credit card data be segregated from the main corporate network to prevent unauthorized access and that access to the IT systems should be logged. Which of the following would BEST meet the CISO's requirements?

- A. Sniffers
- B. NIDS
- C. Firewalls
- D. Web proxies
- E. Layer 2 switches

Correct Answer: C

QUESTION 9

All of the following are encryption types EXCEPT:

- A. Full disk
- B. SMIME
- C. File and folder
- D. RADIUS

Correct Answer: D

QUESTION 10

A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user's host:

Old `hosts` file:

127.0.0.1 localhost New `hosts` file:

127.0.0.1 localhost

5.5.5.5 www.comptia.com

Which of the following attacks has taken place?



- A. Spear phishing
- B. Pharming
- C. Phishing
- D. Vishing

Correct Answer: B

QUESTION 11

Which of the following should Jane, the security administrator, do FIRST when an employee reports the loss of a corporate mobile device?

- A. Remotely lock the device with a PIN
- B. Enable GPS location and record from the camera
- C. Remotely uninstall all company software
- D. Remotely initiate a device wipe

Correct Answer: D

QUESTION 12

An auditor's report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditor's finding?

- A. Disable unnecessary contractor accounts and inform the auditor of the update.
- B. Reset contractor accounts and inform the auditor of the update.
- C. Inform the auditor that the accounts belong to the contractors.
- D. Delete contractor accounts and inform the auditor of the update.

Correct Answer: A

QUESTION 13

Which of the following consists of peer assessments that help identify security threats and vulnerabilities?

- A. Risk assessment
- B. Code reviews



- C. Baseline reporting
- D. Alarms

Correct Answer: B

QUESTION 14

After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

- A. To allow load balancing for cloud support
- B. To allow for business continuity if one provider goes out of business
- C. To eliminate a single point of failure
- D. To allow for a hot site in case of disaster
- E. To improve intranet communication speeds

Correct Answer: BC

QUESTION 15

While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

- A. no longer used to authenticate to most wireless networks.
- B. contained in certain wireless packets in plaintext.
- C. contained in all wireless broadcast packets by default.
- D. no longer supported in 802.11 protocols.

Correct Answer: B

QUESTION 16

Which of the following is best practice to put at the end of an ACL?

- A. Implicit deny
- B. Time of day restrictions
- C. Implicit allow
- D. SNMP string



Correct Answer: A

QUESTION 17

Management has been informed of an increased number of tailgating violations into the server room. Which of the following is the BEST method of preventing future violations?

- A. Security Guards
- B. Man Traps
- C. Proximity Cards
- D. Biometrics authentication

Correct Answer: B

QUESTION 18

A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match. Which of the following describes how the employee is leaking these secrets?

- A. Social engineering
- B. Steganography
- C. Hashing
- D. Digital signatures

Correct Answer: B

QUESTION 19

A group policy requires users in an organization to use strong passwords that must be changed every 15 days. Joe and Ann were hired 16 days ago. When Joe logs into the network, he is prompted to change his password; when Ann logs into the network, she is not prompted to change her password. Which of the following BEST explains why Ann is not required to change her password?

- A. Ann's user account has administrator privileges.
- B. Joe's user account was not added to the group policy.
- C. Ann's user account was not added to the group policy.
- D. Joe's user account was inadvertently disabled and must be re-created.

Correct Answer: C



QUESTION 20

One of the most basic ways to protect the confidentiality of data on a laptop in the event the device is physically stolen is to implement which of the following?

- A. File level encryption with alphanumeric passwords
- B. Biometric authentication and cloud storage
- C. Whole disk encryption with two-factor authentication
- D. BIOS passwords and two-factor authentication

Correct Answer: C

QUESTION 21

Joe, an administrator, installs a web server on the Internet that performs credit card transactions for customer payments. Joe also sets up a second web server that looks like the first web server. However, the second server contains fabricated files and folders made to look like payments were processed on this server but really were not. Which of the following is the second server?

- A. DMZ
- B. Honeynet
- C. VLAN
- D. Honeypot

Correct Answer: D

QUESTION 22

A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

- A. Logic bomb.
- B. Backdoor.
- C. Adware application.
- D. Rootkit.

Correct Answer: B

QUESTION 23



A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another?

- A. Implement a virtual firewall
- B. Install HIPS on each VM
- C. Virtual switches with VLANs
- D. Develop a patch management guide

Correct Answer: C

QUESTION 24

The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) is to: (Select TWO).

- A. Permit redirection to Internet-facing web URLs.
- B. Ensure all HTML tags are enclosed in angle brackets, e.g., "<".
- C. Validate and filter input on the server side and client side.
- D. Use a web proxy to pass website requests between the user and the application.
- E. Restrict and sanitize use of special characters in input and URLs.

Correct Answer: CE

QUESTION 25

The string:

` or 1=1--

represents which of the following?

- A. Bluejacking
- B. Rogue access point
- C. SQL Injection
- D. Client-side attacks

Correct Answer: C

QUESTION 26

A system administrator has noticed vulnerability on a high impact production server. A recent update was made



available by the vendor that addresses the vulnerability but requires a reboot of the system afterwards. Which of the following steps should the system administrator implement to address the vulnerability?

- A. Test the update in a lab environment, schedule downtime to install the patch, install the patch and reboot the server and monitor for any changes
- B. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the patch, and monitor for any changes
- C. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the update, reboot the server, and monitor for any changes
- D. Backup the server, schedule downtime to install the patch, installs the patch and monitor for any changes

Correct Answer: C

QUESTION 27

A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

- A. LDAP
- B. RADIUS
- C. Kerberos
- D. XTACACS

Correct Answer: C

QUESTION 28

Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is \$300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

- A. \$1,500
- B. \$3,750
- C. \$15,000
- D. \$75,000

Correct Answer: B

QUESTION 29

Which of the following must be kept secret for a public key infrastructure to remain secure?



- A. Certificate Authority
- B. Certificate revocation list
- C. Public key ring
- D. Private key

Correct Answer: D

QUESTION 30

Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

- A. SSLv2
- B. SSHv1
- C. RSA
- D. TLS

Correct Answer: D

QUESTION 31

A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Safety

Correct Answer: D

QUESTION 32

Environmental control measures include which of the following?

- A. Access list
- B. Lighting
- C. Motion detection
- D. EMI shielding



Correct Answer: D

QUESTION 33

A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

- A. User assigned privileges
- B. Password disablement
- C. Multiple account creation
- D. Group based privileges

Correct Answer: D

QUESTION 34

Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network?

- A. Security logs
- B. Protocol analyzer
- C. Audit logs
- D. Honeypot

Correct Answer: D

QUESTION 35

Separation of duties is often implemented between developers and administrators in order to separate which of the following?

- A. More experienced employees from less experienced employees
- B. Changes to program code and the ability to deploy to production
- C. Upper level management users from standard development employees
- D. The network access layer from the application access layer

Correct Answer: B

QUESTION 36



Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

- A. 22
- B. 139
- C. 443
- D. 3389

Correct Answer: D

QUESTION 37

Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO).

- A. Rootkit
- B. Logic Bomb
- C. Botnet
- D. Backdoor
- E. Spyware

Correct Answer: BD

QUESTION 38

A security administrator has implemented a policy to prevent data loss. Which of the following is the BEST method of enforcement?

- A. Internet networks can be accessed via personally-owned computers.
- B. Data can only be stored on local workstations.
- C. Wi-Fi networks should use WEP encryption by default.
- D. Only USB devices supporting encryption are to be used.

Correct Answer: D

QUESTION 39

A team of firewall administrators have access to a `master password list` containing service account passwords. Which of the following BEST protects the master password list?



- A. File encryption
- B. Password hashing
- C. USB encryption
- D. Full disk encryption

Correct Answer: A

QUESTION 40

A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?

- A. Group base privileges
- B. Generic account prohibition
- C. User access review
- D. Credential management

Correct Answer: A

[Latest SY0-301 Dumps](#)

[SY0-301 Practice Test](#)

[SY0-301 Brindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.passapply.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © passapply, All Rights Reserved.