SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

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

Correct Answer: C

QUESTION 2

A software company has a shared codebase for multiple projects using the following strategy:

1.

Unused features are deactivated but still present on the code.

2.

New customer requirements trigger additional development work.

Which of the following will most likely occur when the company uses this strategy?

A. Malicious code

B. Dead code

C. Outsourced code

D. Code obfuscation

Correct Answer: B

Dead code refers to portions of a program\\'s source code that are never executed during the program\\'s runtime. In this strategy, features that are deactivated but still present in the code are effectively dead code. They are not actively used or executed, yet they remain in the codebase.

QUESTION 3

An organization\\'s finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy\\'s requirement? (Select TWO).

A. Corrective

B. Deterrent

C. Preventive

D. Mandatory vacations

E. Job rotation

F. Separation of duties

Correct Answer: DE

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. Type squatting

C. Impersonation

D. Watering-hole attack

Correct Answer: D

It\\'s really the only logical answer. Everything else is more plausible to eliminate.

Information elicitation is done directly in-person, meaning it\\'s typically conversational in nature.

Impersonation centers around PERSONS, not websites. You can\\'t impersonate websites; you can only create similar-looking ones.

Water-hole attacks are performed on third-party websites one suspects the targeted organization uses; this can\\'t be the case here if the attacker created the website themselves.

That leaves typosquatting. While it doesn\\'t explicitly say it\\'s a misspelling of another website, we can\\'t outright rule out that possibility either. It\\'s literally the only applicable answer for creating a website that imitates a legitimate one, after all,

and it implies it\\'s not the original site by saying it\\'s emulating the "look and feel of a legitimate website."

Either way, it\\'s ridiculously ambiguous. I\\'m hoping CompTIA weights answers so that not ALL of them award zero points.

Reference:

https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting

QUESTION 5

Which of the following employee roles is responsible for protecting an organization\\'s collected personal information?

A. CTO

B. DPO

C. CEO

D. DBA

Correct Answer: B

Many companies also have a data protection officer or DPO. This is a higher-level manager who is responsible for the organization\\'s overall data privacy policies. https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/dataroles-and-responsibilities/#:~:text=Many%20companies%20also%20have%20a,organization\\'s%20overall%20data%20privacy%20policies.

QUESTION 6

Which of the following should a data owner require all personnel to sign to legally protect intellectual property?

A. An NDA

B. An AUP

C. An ISA

D. An MOU

Correct Answer: A

QUESTION 7

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

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

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

A. SQL injection

B. Cross-site scripting

C. Pass-the-hash

D. Directory traversal

Correct Answer: D

the attacker manipulates the URL parameters by using "../" sequences or absolute file paths to navigate to parent

directories and access arbitrary files and directories on the URL parameter "show" contains multiple "../" sequences, indicating an attempt to navigate to parent directories. The attacker is trying to access the "/etc/passwd" file, which is a commonly targeted file that stores user account information on Unix-based systems.

QUESTION 8

Which of the following are common VoIP-associated vulnerabilities? (Choose two).

A. SPIM

B. Vishing

C. VLAN hopping

D. Phishing

E. DHCP snooping

F. Tailgating

Correct Answer: AB

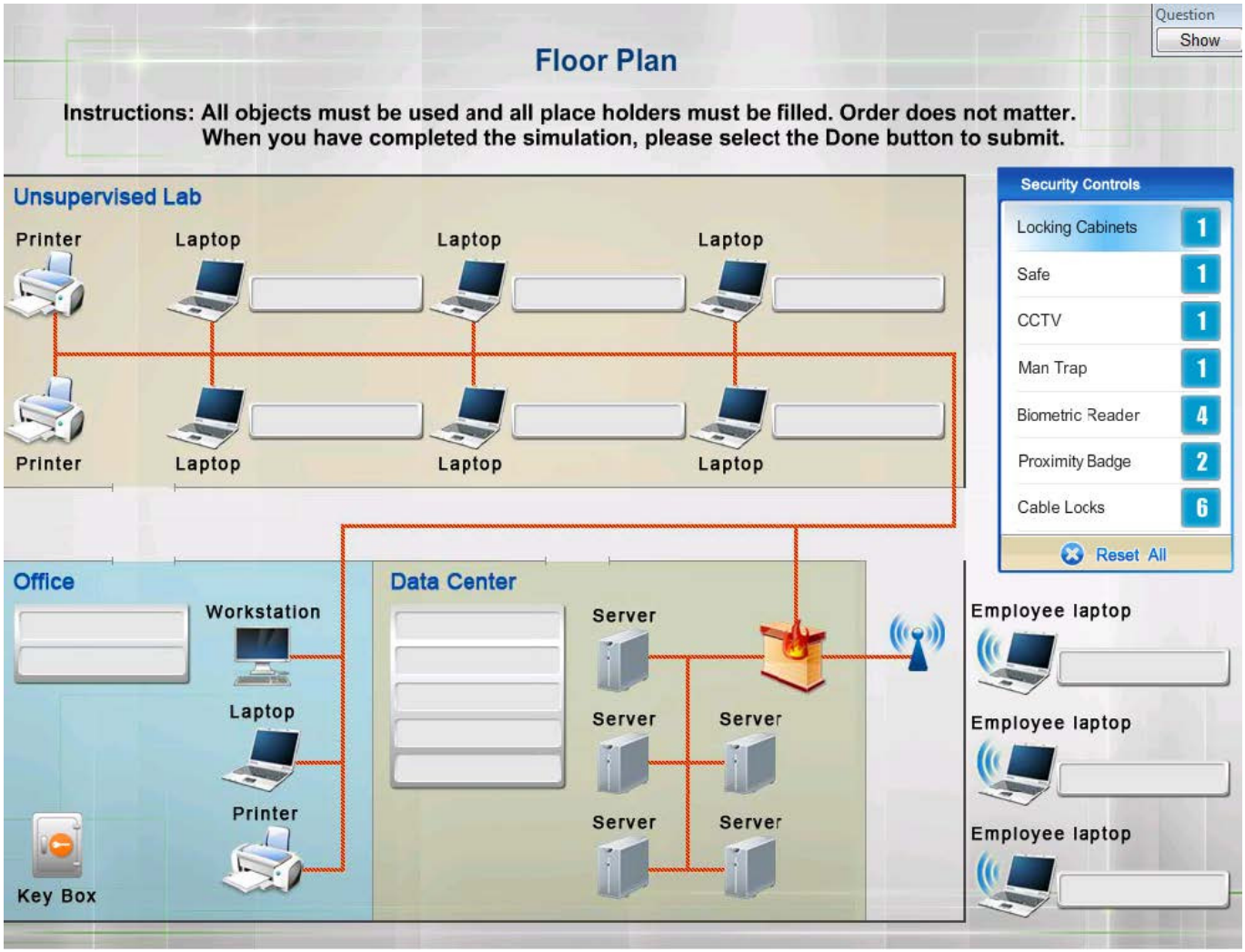
SPIM (Spam over Internet Messaging) poses a threat to VoIP systems by consuming bandwidth, diverting resources, and potentially causing denial of service attacks. The influx of SPIM messages can degrade the quality of VoIP calls, overload servers, and serve as a platform for social engineering attacks, jeopardizing the security of VoIP users. To mitigate these risks, organizations should implement spam filters, intrusion detection systems, and regular software updates while also educating users to recognize and avoid potential threats associated with SPIM.

QUESTION 9

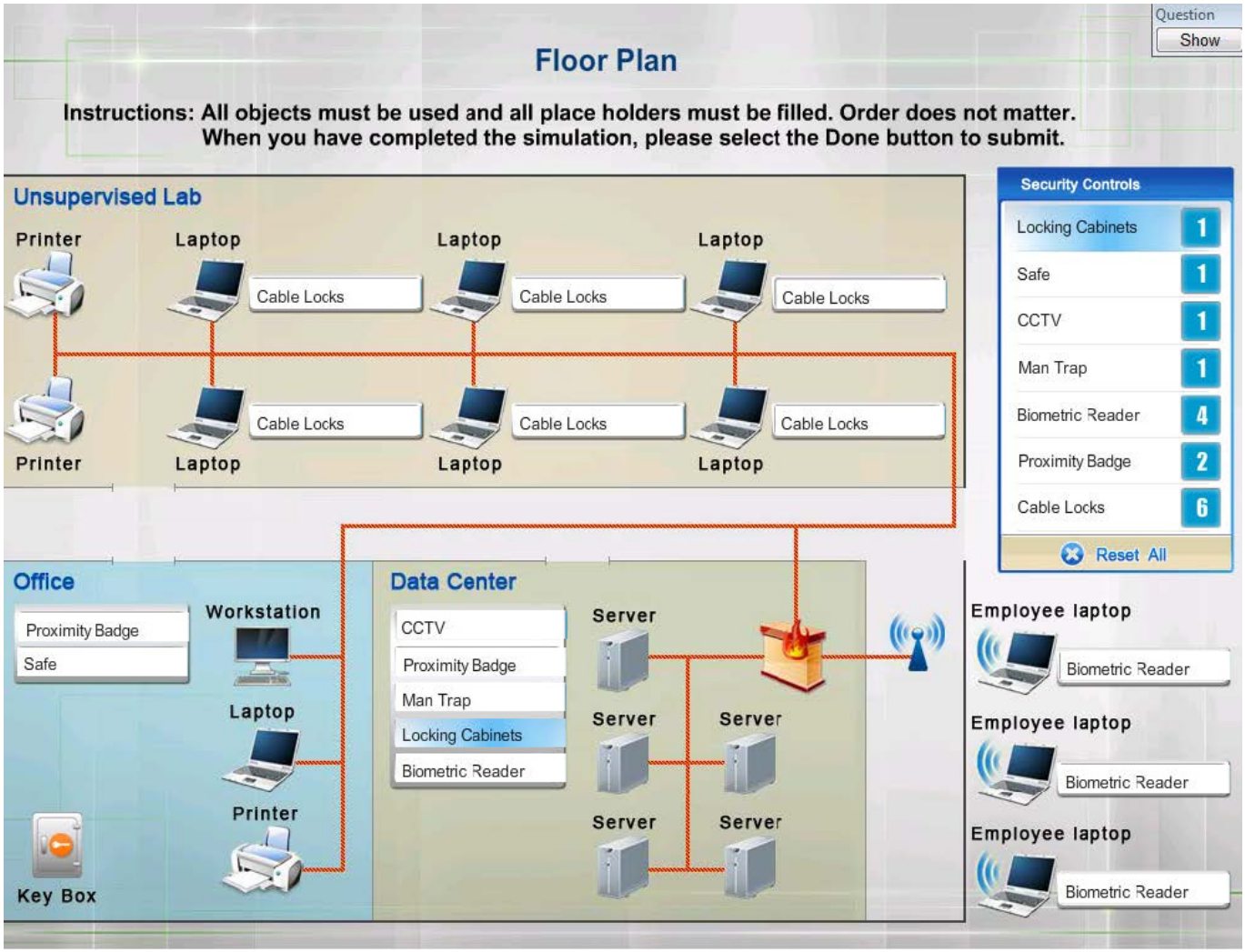
DRAG DROP

You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan-Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

Select and Place:



Correct Answer:



Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away

Proximity badge + reader

Safe is a hardware/physical security measure

Mantrap can be used to control access to sensitive areas.

CCTV can be used as video surveillance.

Biometric reader can be used to control and prevent unauthorized access.

Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 369

QUESTION 10

A penetration tester executes the command crontab -l while working in a Linux server environment. The penetration

tester observes the following string in the current user\\'s list of cron jobs:

*/10 * * * * root /writable/update.sh

Which of the following actions should the penetration tester perform NEXT?

A. Privilege escalation

B. Memory leak

C. Directory traversal

D. Race condition

Correct Answer: A

QUESTION 11

The Chief information Security Officer wants to prevent exfilitration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the Best solution to implement?

A. DLP

B. USB data blocker

C. USB OTG

D. Disabling USB ports

Correct Answer: B

A USB data blocker prevents attackers from infecting a device with malware or stealing data.

When charging your phone in locations such as airports, or other unknown power sources, the use of a USB data blocker protects the phone but allows it to charge

QUESTION 12

A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS

B. ISO 22301

C. ISO 27001

D. NIST CSF

Correct Answer: A

Additionally, many organizations should abide by certain standards. For example, organizations handling credit card

information need to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes six control objectives and 12 specific requirementsthat help prevent fraud

QUESTION 13

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

Correct Answer: A

This is from chapter Authentication and Authorization, The false rejection rate (FRR) determines level false negatives, or rejections

QUESTION 14

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

Correct Answer: B

Heat maps directly correlate to wireless technology. A network diagram isn\\'t specific to wireless, and isn\\'t going to solve the issue.

QUESTION 15

A customer called a company\\'s security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following

1.

The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.

2.

One of the websites the manager used recently experienced a data breach

3.

The manager\\'s corporate email account was successfully accessed in the last five days by an IP address located in a foreign country

Which of the following attacks has MOST likely been used to compromise the manager\\'s corporate account?

A. Remote access Trojan

B. Brute-force

C. Dictionary

D. Credential stuffing

E. Password spraying

Correct Answer: D

"Credential stuffing is a type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames or email addresses and the corresponding passwords (often from a data breach), and then uses the credentials to gain unauthorized access to user accounts"