



Vendor: CompTIA

Exam Code: SY0-401

Exam Name: CompTIA Security+ Certification Exam

Version: DEMO

Added 15 Simulator Questions and New Questions into Full Version

QUESTION 1

Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

- A. Protocol analyzer
- B. Vulnerability scan
- C. Penetration test
- D. Port scanner

Answer: B

Explanation:

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION 2

Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

- A. Cloud computing
- B. Virtualization
- C. Redundancy
- D. Application control

Answer: B

Explanation:

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

QUESTION 3

A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion. Which of the following technologies would BEST be suited to accomplish this?

- A. Transport Encryption
- B. Stream Encryption
- C. Digital Signature
- D. Steganography

Answer: D

Explanation:

Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

QUESTION 4

Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

- A. War chalking
- B. Bluejacking
- C. Bluesnarfing
- D. Rogue tethering

Answer: B

Explanation:

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

QUESTION 5

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

- A. An ephemeral key was used for one of the messages
- B. A stream cipher was used for the initial email; a block cipher was used for the reply
- C. Out-of-band key exchange has taken place
- D. Asymmetric encryption is being used

Answer: D

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION 6

Drag and Drop Question

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.

Question
Show

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.

Unsupervised Lab

Printer Laptop Laptop Laptop
Printer Laptop Laptop Laptop

Security Controls

Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Reset All

Office

Workstation
Laptop
Printer
Key Box

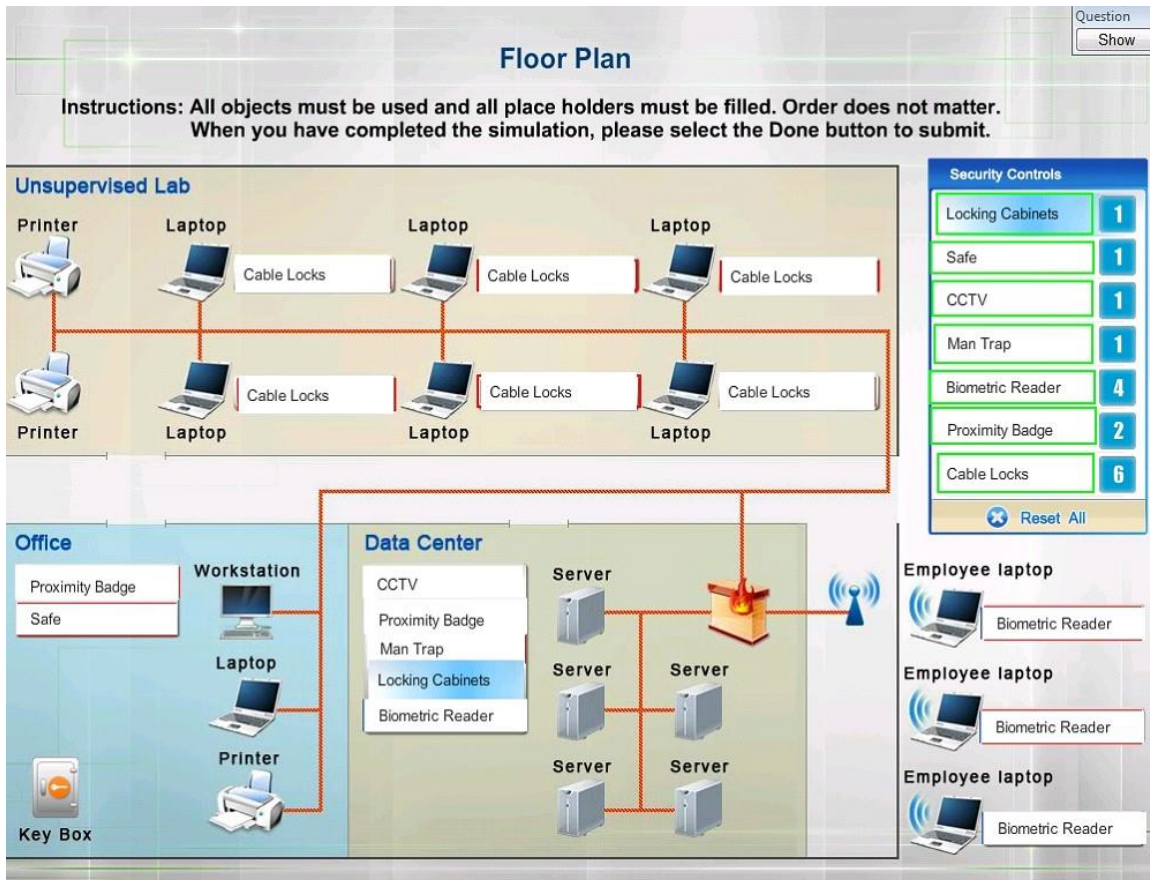
Data Center

Server Server
Server Server
Server Server

Employee laptop

Employee laptop
Employee laptop
Employee laptop

Answer:



QUESTION 7

An administrator needs to connect a router in one building to a router in another using Ethernet. Each router is connected to a managed switch and the switches are connected to each other via a fiber line. Which of the following should be configured to prevent unauthorized devices from connecting to the network?

- A. Configure each port on the switches to use the same VLAN other than the default one
- B. Enable VTP on both switches and set to the same domain
- C. Configure only one of the routers to run DHCP services
- D. Implement port security on the switches

Answer: D

Explanation:

Port security in IT can mean several things:

The physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port.

The management of TCP and User Datagram Protocol (UDP) ports. If a service is active and assigned to a port, then that port is open.

All the other 65,535 ports (of TCP or UDP) are closed if a service isn't actively using them.

Port knocking is a security system in which all ports on a system appear closed. However, if the client sends packets to a specific set of ports in a certain order, a bit like a secret knock, then the desired service port becomes open and allows the client software to connect to the service.

QUESTION 8

The datacenter design team is implementing a system, which requires all servers installed in racks to face in a predetermined direction. AN infrared camera will be used to verify that servers are properly racked. Which of the following datacenter elements is being designed?

- A. Hot and cold aisles
- B. Humidity control
- C. HVAC system
- D. EMI shielding

Answer: A

Explanation:

There are often multiple rows of servers located in racks in server rooms.

The rows of servers are known as aisles, and they can be cooled as hot aisles and cold aisles.

With a hot aisle, hot air outlets are used to cool the equipment, whereas with cold aisles, cold air intake is used to cool the equipment. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation.

Infrared cameras are heat detection measures thus it is hot and cold aisle design elements.

QUESTION 9

Joe, an employee is taking a taxi through a busy city and starts to receive unsolicited files sent to his Smartphone. Which of the following is this an example of?

- A. Vishing
- B. Bluejacking
- C. War Driving
- D. SPIM
- E. Bluesnarfing

Answer: B

Explanation:

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters. Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

QUESTION 10

Which of the following is being tested when a company's payroll server is powered off for eight hours?

- A. Succession plan
- B. Business impact document
- C. Continuity of operations plan
- D. Risk assessment plan

Answer: C

Explanation:

Continuity of operations plan is the effort to ensure the continued performance of critical business functions during a wide range of potential emergencies.

QUESTION 11

An employee recently lost a USB drive containing confidential customer data. Which of the following controls could be utilized to minimize the risk involved with the use of USB drives?

- A. DLP
- B. Asset tracking
- C. HSM
- D. Access control

Answer: A

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

QUESTION 12

A security manager must remain aware of the security posture of each system. Which of the following supports this requirement?

- A. Training staff on security policies
- B. Establishing baseline reporting
- C. Installing anti-malware software
- D. Disabling unnecessary accounts/services

Answer: B

Explanation:

The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline. A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

QUESTION 14

Which of the following concepts is used by digital signatures to ensure integrity of the data?

- A. Non-repudiation
- B. Hashing
- C. Transport encryption
- D. Key escrow

Answer: B

Explanation:

Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad.**
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives®

10% Discount Coupon Code: ASTR14