



Vendor: Cisco

Exam Code: 100-160

Exam Name: Cisco Certified Support Technician (CCST)
Cybersecurity

Version: DEMO

QUESTION 1

Why is it necessary to update firmware to the latest version?

- A. To support the latest operating systems and applications
- B. To patch firmware in the kernel of the operating system
- C. To correct security holes and weaknesses
- D. To explore new hardware features

Answer: C

Explanation:

Keeping firmware up to date is necessary to patch security vulnerabilities and weaknesses that could be exploited by threat actors. Vendors release firmware updates to correct security flaws, enhance stability, and ensure compatibility with updated security protocols.

QUESTION 2

How do threat actors launch ransomware attacks on organizations?

- A. They implant malware to collect data from the corporation's financial system.
- B. They deface an organization's public-facing website.
- C. They lock data and deny access to the data until they receive money.
- D. They secretly spy on employees and collect employees' personal information.

Answer: C

Explanation:

Ransomware is a type of malware that denies access to data by encrypting it and demands payment from the victim to restore access. Threat actors may deliver ransomware through phishing emails, malicious downloads, or exploiting vulnerabilities in exposed systems.

QUESTION 3

You are planning to work from home. Your company requires that you connect to the company network through a VPN.

Which three critical functions do VPNs provide to remote workers? (Choose three.)

- A. WAN management
- B. Authorization of users
- C. Integrity of data
- D. Authentication of users
- E. Confidentiality of information
- F. Password management

Answer: CDE

Explanation:

Authentication of users: VPNs verify the identity of users to ensure only authorized individuals can access the company network.

Integrity of data: VPNs ensure the data transmitted between the remote worker and company network is not altered or tampered with.

Confidentiality of information: VPNs encrypt data to keep it private and protect sensitive information from being intercepted by unauthorized parties.

QUESTION 4

A threat actor sets up a rogue access point (AP) at a local cafe. The rogue AP captures traffic

and then forwards the traffic to the cafe AP.
Which type of attack does this scenario describe?

- A. Reconnaissance
- B. Man-in-the-middle
- C. DDoS
- D. Ransomware

Answer: B

Explanation:

In a MITM attack, the attacker places themselves between the sender and receiver, intercepting and possibly altering data in transit. Rogue access points can facilitate MITM attacks in wireless environments.

QUESTION 5

What is the main purpose of a disaster recovery plan as compared to a business continuity plan?

- A. Limiting operational downtime.
- B. Keeping the business open in some capacity during a disaster.
- C. Restoring data access and an IT infrastructure as quickly as possible.
- D. Allowing staff to continue to serve customers throughout a disaster.

Answer: C

Explanation:

A disaster recovery plan outlines procedures for restoring data and critical IT infrastructure to operational status following a disruptive incident. The goal is to resume normal IT operations as quickly as possible.

QUESTION 6

A restaurant installs a second wireless router that only employees can use. Which statement describes how to securely configure the new router?

- A. Configure the new router to filter IP addresses.
- B. Configure the SSID with broadcast disabled.
- C. Configure a higher signal strength to allow coverage in the parking lot.
- D. Configure the SSID with the same SSID used by the customer router.

Answer: B

Explanation:

Disabling SSID broadcast can reduce the visibility of a wireless network, making it less likely to be detected by casual attackers. This should be combined with strong encryption and authentication.

QUESTION 7

You need to transfer configuration files to a router across an unsecured network. Which protocol should you use to encrypt the files in transit?

- A. Telnet
- B. HTTP
- C. TFTP

D. SSH

Answer: D

Explanation:

SSH encrypts all data exchanged between client and server, protecting credentials and file contents from interception. It is the preferred protocol for secure device management and file transfers across untrusted networks.

QUESTION 8

Hotspot Question

For each statement, select True if it is a common motivation to commit cyber attacks or False if it is not.

Note: You will receive partial credit for each correct selection.

Answer Area		True	False
A person becomes disgruntled at work.	☐	☐	
A person wants to protect personal data.	☐	☐	
A person wants to advance a social agenda.	☐	☐	

Answer:

Answer Area		True	False
A person becomes disgruntled at work.	☒	☐	
A person wants to protect personal data.	☐	☒	
A person wants to advance a social agenda.	☒	☐	

QUESTION 9

Drag and Drop Question

Move each definition from the list on the left to the correct CIA Triad term on the right.

Note: You will receive partial credit for each correct answer.

Definitions	Terms
Legitimate requests should have access to data at all times.	Confidentiality Definition
Data should never be altered or compromised.	Integrity Definition
Data should be accessed and read only by authorized users.	Availability Definition

Answer:

Definitions	Terms
	Confidentiality
	Integrity
	Availability

Data should be accessed and read only by authorized users.
Data should never be altered or compromised.
Legitimate requests should have access to data at all times.

QUESTION 10

Which encryption type is commonly used to secure WiFi networks?

- A. Data Encryption Standard (DES)
- B. Triple Data Encryption Algorithm (Triple DES)
- C. Advanced Encryption Algorithm (AES)
- D. RSA (Rivest-Shamir-Adleman)

Answer: C

Explanation:

WPA2 and WPA3 use the Advanced Encryption Standard (AES) for securing wireless traffic. AES provides strong symmetric encryption, replacing outdated methods like WEP and TKIP.

QUESTION 11

How does sandboxing help with the analysis of malware?

- A. It defines the suspicious or malicious applications that should be blocked.
- B. It specifies the applications that are authorized for use on the network.
- C. It allows suspicious applications to run in a safe and isolated testing environment.
- D. It restricts traffic from passing from one network to another.

Answer: C

Explanation:

Sandboxing isolates a suspected application in a secure, controlled environment where it can be executed and analyzed without risking damage to the host system or network.

QUESTION 12

Which network security technology passively monitors network traffic and compares the captured packet stream with known malicious signatures?

- A. IDS
- B. IPS
- C. Proxy Server
- D. Honeypot

Answer: A

Explanation:

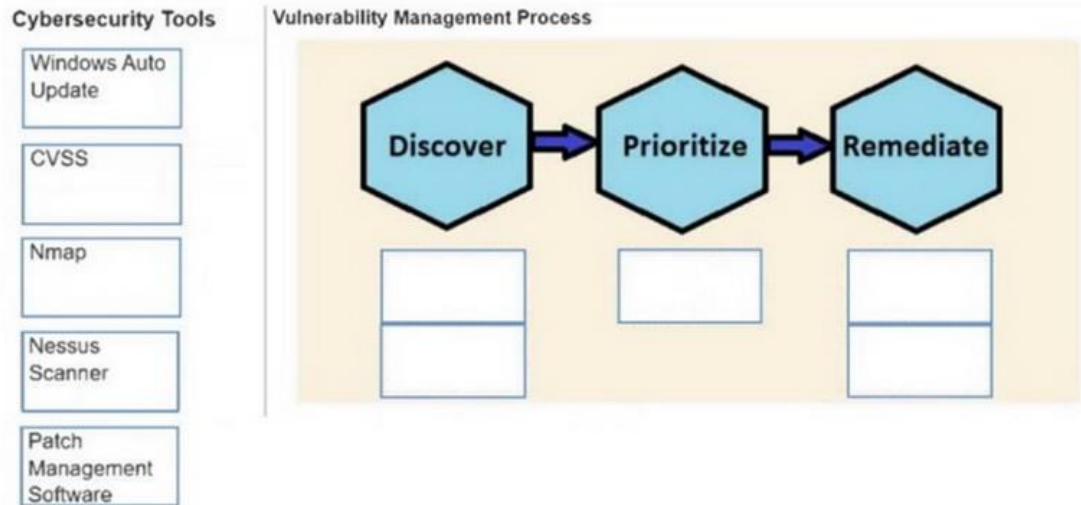
IDS devices inspect network traffic, compare it to known malicious signatures or anomalies, and generate alerts for suspicious activity without actively blocking traffic.

QUESTION 13

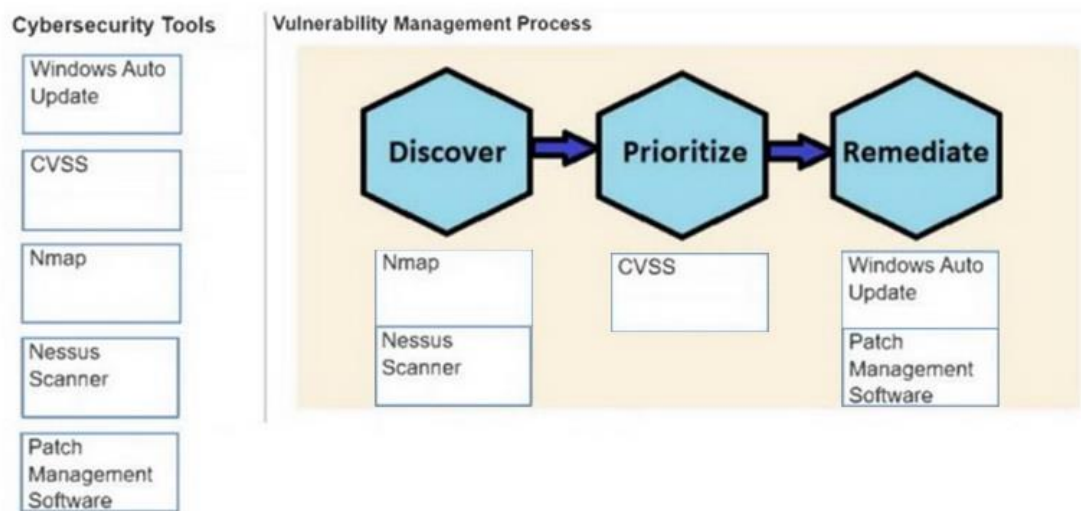
Drag and Drop Question

Move each cybersecurity tool from the list on the left to the correct location on the Vulnerability Management Process diagram on the right.

Note: You will receive partial credit for each correct response.



Answer:



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>



10% Discount Coupon Code: ASTR14