Question 1
Which of the following are steps in the vulnerability management process. Select two answers. 1 / 1 point

<mark>Identify vulnerabilities</mark>

Correct

Vulnerability management is an internal process that includes identifying vulnerabilities and preparing defenses against threats.

Assign a CVE® ID

<mark>Prepare defenses against threats</mark>

Correct

Vulnerability management is an internal process that includes identifying vulnerabilities and preparing defenses against threats.

Catalog organizational assets

Question 2
An organization is attacked by a vulnerability that was previously unknown. What is this exploit an example of? 1 / 1 point

An asset

A perimeter layer

A cipher

<mark>A zero-day</mark>

Correct

A zero-day refers to an exploit that was previously unknown.

Question 3
Which layer of the defense in depth strategy is a user authentication layer that mainly filters external access? 1 / 1 point

<mark>Perimeter</mark>

Data

Network

Endpoint

Correct

The perimeter layer consists of authentication technologies that let verified users in.

Question 4
A security researcher reports a new vulnerability to the CVE® list. Which of the following criteria must the vulnerability meet before it receives a CVE® ID? Select two answers. 1 / 1 point

It must affect multiple applications.

<mark>It must be independently fixable.</mark>

Correct

Criteria that must be met are that vulnerabilities should be independently fixable and must have supporting evidence.

The vulnerability must be unknown to the developer.

<mark>The submission must have supporting evidence.</mark>

Correct

Criteria that must be met are that vulnerabilities should be independently fixable and must have supporting evidence.