Tara is concerned about staff in her organization sending email with sensitive information like customer Social Security numbers (SSNs) included in it. What type of solution can she implement to help prevent inadvertent exposures of this type of sensitive data?

Step 1: Answer with Explanation

Answer: DLP

Explanation:

Data loss prevention, or DLP, is a cybersecurity tool that tracks down and stops data breaches. Organizations use it for internal security and regulatory compliance since it prevents sensitive data from being extracted. Data loss prevention (DLP) is the process of identifying and stopping sensitive data breaches, exfiltration, and unintentional deletion.

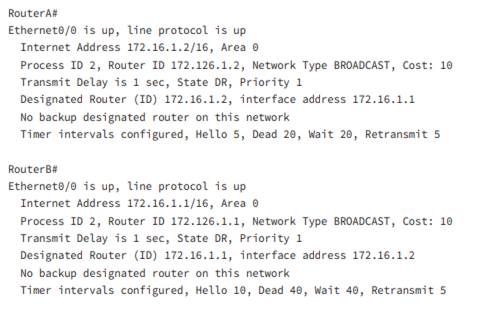
Step 2: Explanation for incorrect option

Full disc encryption (FDE) is a security measure that uses disk-level encryption to shield all data stored on a hard drive from unauthorised access. With FDE, all data is encrypted by default, removing the user's control over security.

Secure/Multipurpose Internet Mail Extensions is referred to as S/MIME. We can use this technology to encrypt the content of our emails, making them resistant to online attacks. In other words, S/MIME keeps our emails secure and ensures that only the intended recipient may view them.

The most used protocol for receiving email over the internet is Post Office Protocol 3, or POP3. This common protocol is used to transmit emails from a remote server to a local client and is supported by the majority of email servers and clients.

For some reason, you cannot establish an adjacency relationship on a common Ethernet link between two routers. Looking at this output, what is the cause of the problem?



A. The OSPF area is not configured properly.

B. The priority on Router A should be set higher.

C. The cost on Router A should be set higher.

D. The Hello and Dead timers are not configured properly.

E. A backup designated router needs to be added to the network.

F. The OSPF process ID numbers must match.

Step 1: Answer

D. The Hello and Dead timers are not configured properly.

Step 2: Explanation

For rerouting Internet Protocol (IP) packets inside a single routing domain, such as an autonomous system, OSPF is an inner gateway protocol (IGP). It creates a topology map of the network by compiling link state data from available routers.

The hello interval in OSPF must be equal to the dead interval, which in this case is set to 5 on R1 and 10 on R2. On R1, the dead interval is also set to 20, whereas on R2, it is 40.

Two routers connected by the same connection must have their Hello and Dead timers set to the same value in order for them to form an adjacency (relationship). The Hello timer for OSPF is set to 10 seconds by default, and the Dead timer is set to 40 seconds.

Charlene is preparing a report on the most common application security issues for cloud applications. Which of the following is not a major concern for cloud applications?

**A.**Local machine access leading to compromise

**B.**Misconfiguration of the application

**C.**Insecure APIs

**D.**Account compromise

Step 1: Answer

**A.**Local machine access leading to compromise

Step 2: Explanation

Any flaws, holes, or faults in the cloud that could put your environment at danger when you use the cloud are referred to as cloud misconfiguration. These cyber threats include security lapses, foreign hackers, ransomware, malware, and insider threats that gain access to your network through vulnerabilities.

A growing threat comes from insecure APIs.

Although APIs are increasingly useful for streamlining cloud computing procedures, they frequently raise security issues, especially if left unprotected. Insecure APIs can be used by adversaries to compromise or steal private and sensitive data.

 Account compromise

An account is compromised when a threat actor obtains access to credentials and/or other methods to carry out acts on behalf of the targeted user, whether it be through social engineering, phishing, or other cyber-attacks.

            Michelle wants to check for authentication failures on a CentOS Linux–based system. Where should she look for these event logs?

**A.**/var/log/auth.log

**B.**/var/log/fail

**C.**/var/log/events

**D.**/var/log/secure

Step 1: Answer

/var/log/faillog -

Contains failed client login endeavors. Use faillog order to show the substance of this document.

Step2: Explanation

The organizer/var/log/messages contain different messages, like mail, kern, auth, cron, daemon, etc. Linux log information is a valuable investigating utility at whatever point you run into issues with the Linux working framework, projects, or server. They give an order of the Linux framework, applications, and structure activities.

/var/log/auth. log -

Contains framework approval data, including client logins and verification machinsm that were utilized.

/var/log/secure -

Contains data connected with verification and approval honors. For instance, sshd logs every one of the messages here, including fruitless login.

 What does the OPAL standard specify?

**A.**Online personal access licenses

**B.**Self-encrypting drives

**C.**The origin of personal accounts and libraries

**D.**Drive sanitization modes for degaussers

Step 1: Answer

**B.**Self-encrypting drives

Step 2: Explanation

The Opal Storage Specification is a set of requirements for security-enhancing characteristics of data storage devices (such disc drives). For instance, it specifies how to encrypt the data stored on the device so that it cannot be accessed by unauthorised individuals.

Opal is the name of a self-encrypting disc specification created by the Trusted Computing Group, a standards organisation. Opal is a specification that outlines the expected behaviour and the commands the drive must comply with.

Data saved in self-encrypting drives (SEDs) that support Opal 2.0 is protected using hardware encryption technology. Users can stop worrying about their data being accessible if their drive, laptop, or mobile device is stolen or lost by encrypting the entire disc.