DISA Assured Compliance Assessment Solution (ACAS) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **Which security center role is responsible for creating an organization?**

   A. Administrator

   B. Security Analyst

   C. Security Manager

   D. Executive

2. **Which type of objects can users in the same group utilize among themselves?**

   A. Reports only

   B. Assets only

   C. Policies only

   D. All selected objects

3. **According to the ACAS contract, how can you get your Tenable.sc plugin updates?**

   A. Automatically from DISA's plugin server

   B. Manually from the DoD Patch Repository

   C. Download a copy from the vendor

   D. All of the above

4. **What is a static asset list?**

   A. A list that defines groups of machines that have common aspects

   B. A list of IP addresses that requires user intervention to change

   C. A list of assets based on passive or active scan results

   D. None of the above

5. **What benefit does ACAS offer regarding federal information security?**

   A. It ensures complete data encryption

   B. It simplifies the compliance processes for federal agencies

   C. It helps achieve compliance with established security standards

   D. It guarantees total absence of data breaches

6. How does ACAS assist organizations during security incidents?

A. By providing detailed user training

B. By offering antivirus software at a discount

C. By providing rapid identification of vulnerabilities that may have been exploited

D. By directly responding to threats on behalf of organizations

7. The Nessus scanner scans data at rest, while the NNM monitors data in motion.

A. True

B. False

C. Sometimes

D. Only with certain configurations

8. In terms of compliance, ACAS aligns with which act?

A. Health Insurance Portability and Accountability Act (HIPAA)

B. Federal Information Security Management Act (FISMA)

C. Globetrotter Security Management Act

D. Payment Card Industry Data Security Standard (PCI DSS)

9. A Nessus Agent is ___.

A. The passive scanner that detects vulnerabilities by sniffing network traffic

B. A lightweight program installed on the endpoint that gives visibility into assets that connect intermittently to the internet.

C. Web Publishing feature gives Tenable.sc the ability to publish reports to target websites

D. A main server that manages and distributes scans

10. How does ACAS differentiate between high, medium, and low vulnerabilities?

A. By assessing the urgency of required actions

B. By evaluating the severity and potential impact of each vulnerability

C. By the number of systems affected

D. By the time since the last vulnerability scan

Answers

1. **A**
2. **D**
3. **A**
4. **B**
5. **C**
6. **C**
7. **A**
8. **B**
9. **B**
10. **B**

Explanations

1. Which security center role is responsible for creating an organization?

A. Administrator

B. Security Analyst

C. Security Manager

D. Executive

The Administrator role in a security center is primarily responsible for setting up and managing the organization's infrastructure within the security system. This encompasses creating and configuring the organization itself, which includes defining the structure, roles, and permissions that are essential for the system's operational effectiveness. The Administrator ensures that the security framework aligns with the organization's policies and compliance requirements. This role is foundational, as it lays the groundwork for how security procedures are implemented and who has access to what within the organization. The effectiveness of the security program is heavily reliant on the Administrator's ability to establish a robust and secure organization setup. As such, the Administrator's tasks often involve not just initial setup, but ongoing management and updates to adapt to new security challenges or structural changes within the organization. The other roles, while integral to the security center's operations, have different focuses; for example, the Security Analyst investigates and responds to security incidents, the Security Manager oversees the security protocols and strategies, and the Executive focuses on high-level oversight, strategic decisions, and stakeholder engagement.

2. Which type of objects can users in the same group utilize among themselves?

A. Reports only

B. Assets only

C. Policies only

D. All selected objects

Users within the same group can utilize various types of objects, which includes reports, assets, and policies. This collaborative functionality is often designed to enhance teamwork and maintain consistency in operations within an organization. When users are part of a shared group, it facilitates their ability to access and manage these objects collectively, thereby promoting a unified approach to security assessments and compliance monitoring. Reports provide insights and data analysis, assets represent the items being managed or protected, and policies outline the guidelines and procedures to follow. Allowing all selected objects to be used among the group enhances resource sharing, improves decision-making, and aligns actions to achieve compliance goals more effectively. This comprehensive access is crucial for ensuring that all members can contribute to their group's objectives while adhering to best practices and regulations.

3. According to the ACAS contract, how can you get your Tenable.sc plugin updates?

A. Automatically from DISA's plugin server

B. Manually from the DoD Patch Repository

C. Download a copy from the vendor

D. All of the above

The correct answer highlights that Tenable.sc plugin updates can be obtained automatically from DISA's plugin server. This method allows for a streamlined and efficient update process, ensuring that users have timely access to the latest security features, vulnerability checks, and enhancements provided by Tenable. By leveraging the automated updates via DISA's dedicated server, users can minimize the risk of operating with outdated plugins, which could expose their environments to potential vulnerabilities. In contrast, manually obtaining updates from the DoD Patch Repository or downloading them directly from the vendor are less efficient and could lead to delays in applying critical updates. The automatic retrieval system is specifically designed to facilitate compliance with DoD policies and maintain a secure posture, making it the preferred method for managing plugin updates in the context of the ACAS framework.

4. What is a static asset list?

A. A list that defines groups of machines that have common aspects

B. A list of IP addresses that requires user intervention to change

C. A list of assets based on passive or active scan results

D. None of the above

A static asset list is indeed best understood as a collection of defined assets, such as a list of IP addresses or identifiers that do not change frequently and require deliberate action to modify. This means that the list is not automatically updated or modified based on real-time data or scans. Users need to actively manage and modify this list when necessary, reflecting the thought that it requires user intervention to change. In contrast, the other options do not accurately describe a static asset list. For instance, a list that defines groups of machines with common aspects pertains more to categorization based on shared attributes rather than a fixed inventory of assets. Additionally, a list based on passive or active scan results suggests a dynamic process where assets are identified automatically, contrasting sharply with the concept of a static list that doesn’t change without manual input. Thus, option B aligns properly with the concept of a static asset list as one that remains unchanged unless actively altered by a user.

5. What benefit does ACAS offer regarding federal information security?

A. It ensures complete data encryption

B. It simplifies the compliance processes for federal agencies

C. It helps achieve compliance with established security standards

D. It guarantees total absence of data breaches

ACAS, the Assured Compliance Assessment Solution, is designed to assist federal agencies in achieving compliance with established security standards. This is a crucial benefit since federal information security requires adherence to numerous regulations and guidelines, such as those set forth by the Federal Information Security Management Act (FISMA) and the NIST (National Institute of Standards and Technology) framework. By offering tools and automated functionalities that help assess security controls, monitor vulnerabilities, and report on compliance status, ACAS facilitates the process of ensuring that federal agencies meet these rigorous standards and maintain a strong security posture. In contrast, while some other options mention aspects related to data and security, they do not encapsulate the primary function of ACAS. Complete data encryption cannot be assured solely by the implementation of ACAS; it is a broader security feature that depends on various technologies and practices. Simplifying compliance processes is a part of what ACAS aims to do, but it specifically emphasizes achieving compliance with security standards as its primary focus. Lastly, ACAS cannot guarantee a total absence of data breaches, as security is influenced by numerous factors outside of ACAS's scope, including user behavior and external threats. Thus, the choice highlighting compliance with established security standards accurately reflects the core benefit of the

6. How does ACAS assist organizations during security incidents?

A. By providing detailed user training

B. By offering antivirus software at a discount

C. By providing rapid identification of vulnerabilities that may have been exploited

D. By directly responding to threats on behalf of organizations

ACAS (Assured Compliance Assessment Solution) plays a critical role in assisting organizations during security incidents primarily by offering rapid identification of vulnerabilities that may have been exploited. In the context of a security incident, the ability to quickly diagnose existing vulnerabilities allows organizations to respond effectively and prioritize their remediation efforts. This rapid identification is vital for limiting the damage caused by a security breach, as it enables organizations to understand which systems and assets are at risk and require immediate attention. The focus of ACAS is on assessing and reporting the compliance status of systems against established security configurations and best practices. When a security incident occurs, having a robust tool like ACAS allows security teams to quickly determine if any previously known vulnerabilities were targeted. This proactive approach helps them to not only mitigate the current threat but also to strengthen their defenses against future attacks. In comparison, options like providing detailed user training, offering antivirus software at a discount, or directly responding to threats miss the essential function of ACAS in vulnerability management during security incidents. While training and software solutions are important components of an overall security posture, they do not address the immediate need for detection and assessment that is critical during or immediately following a security incident.

7. The Nessus scanner scans data at rest, while the NNM monitors data in motion.

A. True

B. False

C. Sometimes

D. Only with certain configurations

The statement is accurate because the Nessus scanner is designed to perform vulnerability assessments on systems by scanning data that is not currently changing, often referred to as data at rest. It evaluates the security posture of systems, applications, and configurations to identify vulnerabilities that could be exploited by attackers. On the other hand, Network Node Manager (NNM) is employed for monitoring network performance and health, which involves observing data as it flows across the network—this is referred to as data in motion. NNM helps in tracking network traffic, ensuring smooth operation, and identifying any anomalies or performance issues in real-time. This clear distinction between the functions of Nessus and NNM supports the statement and showcases how both tools serve essential and complementary roles in security monitoring and management within a network environment.

8. In terms of compliance, ACAS aligns with which act?

A. Health Insurance Portability and Accountability Act (HIPAA)

B. Federal Information Security Management Act (FISMA)

C. Globetrotter Security Management Act

D. Payment Card Industry Data Security Standard (PCI DSS)

The Federal Information Security Management Act (FISMA) is the correct alignment for ACAS in terms of compliance. FISMA establishes a framework for ensuring the effectiveness of information security controls across federal agencies and their contractors. This act requires these entities to secure their information systems and conduct annual audits, which aligns with ACAS's purpose of assessing compliance with security controls and vulnerabilities.   The framework provided by FISMA supports the overall mission of ACAS, which is to ensure that the security posture of federal information systems meets the stipulated regulatory standards. By focusing on risk management and continuous monitoring, ACAS operates under the guidelines set forth by FISMA, integrating it into federal compliance initiatives.   Understanding FISMA's role is crucial as it forms the backbone of federal information security policy, and ACAS serves as a tool to validate and ensure adherence to the requirements set by this act. This synergy highlights the importance of FISMA in governing how security assessments are conducted under ACAS.

9. A Nessus Agent is ___.

A. The passive scanner that detects vulnerabilities by sniffing network traffic

B. A lightweight program installed on the endpoint that gives visibility into assets that connect intermittently to the internet.

C. Web Publishing feature gives Tenable.sc the ability to publish reports to target websites

D. A main server that manages and distributes scans

A Nessus Agent is indeed a lightweight program installed on endpoints, which provides critical visibility into assets that may connect to the internet intermittently. This capability is essential in modern network environments where devices often operate outside the traditional bounds of the corporate firewall and may not be consistently accessible for scanning. The Nessus Agent allows for continuous monitoring of these endpoints, gathering information about vulnerabilities, compliance, and configurations irrespective of their network connection status at any given time. This is particularly beneficial for organizations with a mobile workforce or those utilizing cloud services, as it ensures that even devices that are not always online can still be assessed for security risks. This approach enhances the overall security posture of an organization by allowing for more frequent and detailed assessments compared to traditional scanning methods that might only occur when devices are connected to a specific network. The Nessus Agents can report back to the central management system when the devices reconnect, thus ensuring that the data collected is timely and relevant. The other options present concepts that don't align with the primary functionality of a Nessus Agent. For instance, a passive scanner relates to techniques that analyze traffic without active scanning, which differs from the proactive nature of agents. Similarly, the feature related to web publishing and the main server managing scans pertains more to the broader

10. How does ACAS differentiate between high, medium, and low vulnerabilities?

A. By assessing the urgency of required actions

B. By evaluating the severity and potential impact of each vulnerability

C. By the number of systems affected

D. By the time since the last vulnerability scan

ACAS differentiates between high, medium, and low vulnerabilities primarily by evaluating the severity and potential impact of each vulnerability. This assessment takes into account various factors, including how easily a vulnerability can be exploited, the potential damage it can cause if exploited, and the overall risk it poses to the organization's systems and data. By systematically categorizing vulnerabilities in this manner, ACAS aids organizations in prioritizing their responses and allocating resources effectively to address the most serious threats first. The urgency of required actions is important but arises from the severity and potential impact analysis rather than being a distinct categorization metric. Similarly, while the number of affected systems can indicate the breadth of an issue, it does not inherently define the gravity of a vulnerability itself. Lastly, the time since the last vulnerability scan could provide context for timing or frequency but does not measure the vulnerability's criticality or potential impact, which is the core of how ACAS classifies them as high, medium, or low. Thus, evaluating severity and impact is the most fundamental criterion for determining vulnerability levels in ACAS.