DUMPSBOSS.

GIAC Critical Controls Certification (GCCC)

GIAC GCCC

Version Demo

Total Demo Questions: 11

Total Premium Questions: 119

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

An organization has implemented a control for Controlled Use of Administrative Privileges. They are collecting audit data for each login, logout, and location for the root account of their MySQL server, but they are unable to attribute each of these logins to a specific user. What action can they take to rectify this?

A. Force the root account to only be accessible from the system console.

B. Turn on SELinux and user process accounting for the MySQL server.

C. Force user accounts to use 'sudo' f or privileged use.

D. Blacklist client applications from being run in privileged mode.

ANSWER: C

Explanation:

Force user accounts to use `sudo` for privileged use. This approach eliminates routine shared use of the root identity and requires each administrator to authenticate with an individually assigned account before elevating privileges. The resulting audit trail can associate a privileged action with the authenticated user, the time of use, and—when system and authentication logs are collected—the originating session or host. This directly supports accountability for administrative activity, which is the key issue when a shared root account prevents the organization from identifying who performed a login or action.

On systems that support it, `sudo` policies can also limit which users may elevate privileges, which commands they may run, and whether additional authentication is required. Logging sudo events centrally and retaining the underlying authentication records provides a more complete and attributable record for privileged MySQL administration. CIS Controls guidance emphasizes using dedicated accounts for administrative activities and maintaining accountability for elevated access. The sudo project documents that sudo logs successful and unsuccessful command executions, while CIS describes the broader access-control objective in its safeguards guidance. See the sudo documentation and the CIS Account Management control guidance.

QUESTION NO: 2

Which of the following assigns a number indicating the severity of a discovered software vulnerability?

A. CPE

B. CVE

C. CCE

D. CVSS

ANSWER: D

Explanation:

CVSS is correct because the Common Vulnerability Scoring System provides a standardized numerical method for expressing the severity of a software vulnerability. A CVSS Base Score ranges from 0.0 to 10.0 and is calculated from technical characteristics such as attack vector, attack complexity, privileges required, user interaction, scope, and the impact to confidentiality, integrity, and availability. This common scoring approach lets vulnerability-management teams consistently prioritize remediation work: a vulnerability with a higher score generally represents greater potential technical impact and urgency than one with a lower score. CVSS can also include Temporal and Environmental metric groups, enabling an organization to refine the score based on factors such as exploit maturity, available remediation, and the affected organization's own environment. The National Vulnerability Database publishes CVSS severity ratings with vulnerability records and describes the corresponding severity ranges. The CVSS specification is maintained by FIRST, which defines the scoring metrics and calculation methodology. See the NIST National Vulnerability Database CVSS metrics guidance and the FIRST CVSS specifications and resources.

QUESTION NO: 3

After installing a software package on several workstations, an administrator discovered the software opened network port TCP 23456 on each workstation. The port is part of a software management function that is not needed on corporate workstations. Which actions would best protect the computers with the software package installed?

A. Document the port number and request approval from a change control group

B. Redirect traffic to and from the software management port to a non-default port

C. Block TCP 23456 at the network perimeter firewall

D. Determine which service controls the software management function and opens the port, and disable it

ANSWER: D

Explanation:

Determine which service controls the software management function and opens the port, and disable it. This is the most effective action because the management function has no business need on the affected workstations, so the secure configuration is to remove the unnecessary listening service rather than merely filter some traffic directed to it. Disabling the responsible service prevents it from accepting connections, reduces the system's attack surface, and eliminates opportunities for vulnerabilities or configuration errors in that service to be exploited. It also aligns with the CIS Critical Security Controls principle of securely configuring enterprise assets and software: organizations should disable or remove unnecessary services, ports, and functionality as part of maintaining hardened system configurations. The action should be performed through authorized configuration-management procedures and validated afterward by confirming that the service is stopped or disabled and that TCP 23456 is no longer listening on each workstation. This approach provides protection regardless of whether an attempted connection originates internally or externally, while retaining an auditable, repeatable workstation baseline. CIS Control 4 specifically addresses secure configuration management and recommends removing or disabling unnecessary services. See the CIS Control 4 overview and the CIS Critical Security Controls.

QUESTION NO: 4

To effectively implement the Data Protection CIS Control, which task needs to be implemented first?

A. The organization's proprietary data needs to be encrypted

B. Employees need to be notified that proprietary data should be protected

C. The organization's proprietary data needs to be identified

D. Appropriate file content matching needs to be configured

ANSWER: C

Explanation:

The organization's proprietary data needs to be identified first. Effective data protection starts with knowing which information the organization possesses, where it resides, who owns it, and how sensitive it is. This identification and classification activity establishes the scope for every subsequent protection decision, including access restrictions, retention requirements, encryption, monitoring, and controls intended to prevent data loss. Without an inventory of sensitive and proprietary data, an organization cannot reliably determine what must receive enhanced safeguards or validate that protections are applied consistently across endpoints, servers, cloud services, and third-party environments.

CIS Control 3, Data Protection, begins by requiring an enterprise-wide process to identify and classify sensitive data. CIS Safeguard 3.1 specifically calls for an established process to identify and classify sensitive data, and it specifies categories such as regulated data, customer data, intellectual property, and other business-sensitive information. Identification is therefore the foundational task that informs selection and configuration of the remaining data-protection measures. The CIS Controls documentation is available through the CIS Data Protection Control page and the CIS Controls v8 resource page.

QUESTION NO: 5

Which of the following is necessary to automate a control for Inventory and Control of

Hardware Assets?

A. A method of device scanning

B. A centralized time server

C. An up-to-date hardening guide

D. An inventory of unauthorized assets

ANSWER: A

Explanation:

A method of device scanning is necessary because an automated hardware-asset inventory control must be able to discover devices that are connected to the organization's environment and compare those findings with the authorized asset inventory. Device scanning can use active discovery techniques, such as network scans and authenticated queries, and may be supplemented by passive discovery sources. The essential capability is automated identification of systems so that newly connected, unmanaged, or otherwise unrecorded hardware can be detected promptly.

This supports the purpose of the Inventory and Control of Hardware Assets safeguard: maintaining visibility into enterprise assets throughout their lifecycle and identifying unauthorized assets before they create unmanaged exposure. Automated discovery provides current evidence rather than relying solely on manually maintained lists, which can become incomplete as endpoints, servers, network equipment, and other devices are added, moved, or removed. CIS Control 1 specifically calls for active discovery tools to identify assets connected to the enterprise and for the results to be reconciled with the asset inventory. See the CIS Control 1 overview and the CIS Critical Security Controls v8 resources.

QUESTION NO: 6

A network administrator is reviewing outbound firewall logs and finds several workstations making DNS requests directly to public Internet resolvers. The organization operates internal DNS resolvers that apply logging and domain filtering. Which action best supports secure network management?

A. Restrict outbound DNS traffic so that clients use the authorized internal resolvers

B. Configure workstations to use any public DNS resolver for redundancy

C. Disable DNS logging on the internal resolvers

D. Allow outbound DNS only during business hours

ANSWER: A

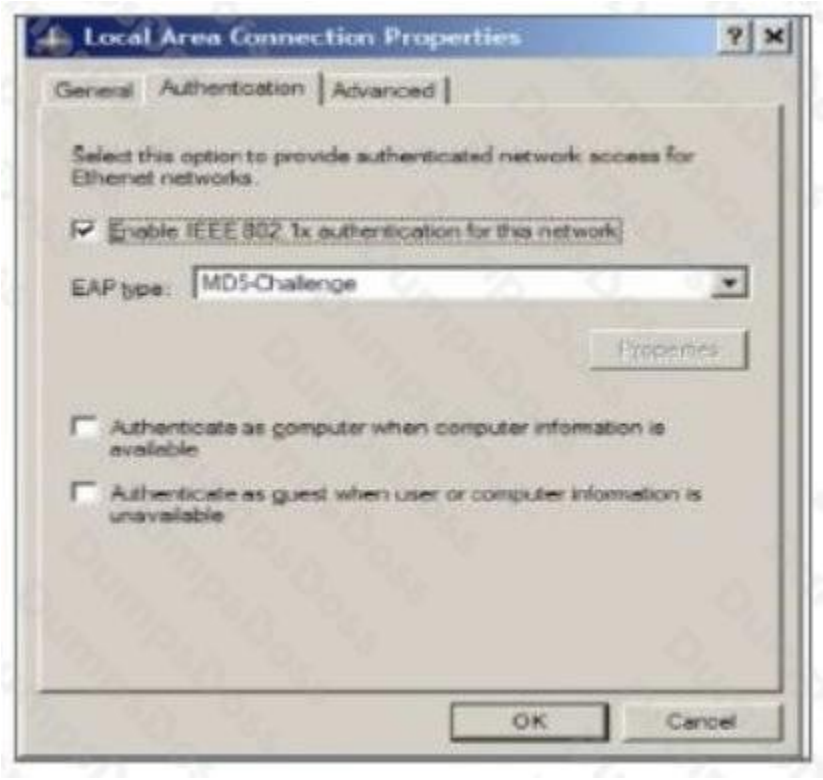
Explanation:

Restrict outbound DNS traffic so that clients use the authorized internal resolvers is correct because it ensures that DNS requests pass through the organization's managed infrastructure. Internal resolvers can log queries, apply threat-intelligence or policy filtering, enforce configuration standards, and provide analysts with useful visibility into suspicious domain lookups.

Allowing endpoints to use arbitrary external resolvers bypasses these controls and can conceal command-and-control lookups or attempts to reach malicious domains. Network filtering should allow the authorized resolver infrastructure to perform external resolution while preventing direct client access to unapproved DNS services. See CIS Control 12: Network Infrastructure Management and NIST SP 800-81 Rev. 2.

QUESTION NO: 7

The settings in the screenshot would be configured as part of which CIS Control?



A. Application Software Security

B. Inventory and Control of Hardware Assets

C. Account Monitoring and Control

D. Controlled Use of Administrative Privileges

ANSWER: B

Explanation:

Inventory and Control of Hardware Assets is correct because the depicted configuration concerns identifying, tracking, and maintaining visibility of devices connected to the organization's environment. Effective hardware-asset inventory processes establish an authorized-device baseline and provide the information needed to detect unmanaged, unknown, or unauthorized systems. This includes maintaining accurate records for enterprise assets, such as workstations, servers, mobile devices, network-connected equipment, and virtualized devices, along with relevant attributes including ownership, location, and operational status.

Hardware inventory is a foundational security activity because many subsequent safeguards depend on knowing which devices exist and whether they are approved to access organizational resources. Asset-discovery and inventory settings support continuous or regularly updated visibility, allowing security teams to reconcile discovered devices against the authorized inventory and respond appropriately when an unrecognized asset appears. In the current CIS Controls structure, this objective is represented by Control 1, Enterprise Asset Inventory. CIS describes this control and its safeguards in the CIS Controls list; its broader purpose and implementation guidance are available through the CIS Controls version 8 resources.

QUESTION NO: 8

Kenya is a system administrator for SANS. Per the recommendations of the CIS Controls she has a dedicated host (kenya-adminbox / 10.10.10.10) for any administrative tasks. She logs into the dedicated host with her domain admin credentials. Which of the following connections should not exist from kenya-adminbox?

```
kenya-adminbox:~ kenya$ netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address                (state)
tcp4       0      0  kenya-adminbox.49722   10.10.10.245.3389              ESTABLISHED
tcp4       0      0  kenya-adminbox.49723   firewall_charon.jane.org.22    ESTABLISHED
tcp4       0      0  kenya-adminbox.49720   mail.jane.org.25               ESTABLISHED
tcp4       0      0  kenya-adminbox.49719   10.10.10.33.443                ESTABLISHED

kenya-adminbox:~ kenya$
```

A. 10.10.245.3389

B. Mail.jane.org.25

C. Firewall_charon.jane.org.22

D. 10.10.10.33.443

ANSWER: B

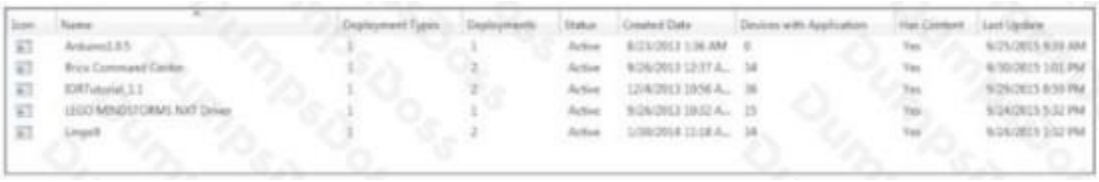
Explanation:

Mail.jane.org.25 is the connection that should not exist. The destination name indicates a mail system, and port 25 is the standard SMTP service port. A dedicated administrative workstation is intended to provide a highly controlled, purpose-specific environment from which privileged users perform administration of enterprise systems. Its network activity should therefore be limited to the management paths and services required for those tasks. Sending mail directly to, or communicating with, an SMTP service is not an administrative-management function and introduces an unnecessary route for exposure, phishing, content handling, and credential compromise on a host where highly privileged domain credentials are used.

CIS Controls guidance for securely managed dedicated administrative workstations emphasizes separating privileged administration from normal user activities. In practice, this means the administrative host should not be used for email, general web browsing, or other productivity functions, and network controls should enforce that restricted purpose. Preventing SMTP connectivity from the administrative host supports this separation and reduces the likelihood that a compromise of a messaging-related workflow can affect a privileged administration environment. See the CIS Controls v8 Navigator for the securely managed dedicated workstation safeguard, and NIST's SP 800-53 for related least-privilege and privileged-access security-control guidance.

QUESTION NO: 9

What is the list displaying?



A. Allowed program in a software inventory application

B. Unauthorized programs detected in a software inventory

C. Missing patches from a patching server

D. Installed software on an end-user device

ANSWER: A

Explanation:

The list is displaying an allowed program in a software inventory application. An authorized-software inventory is used to maintain a defined set of software that the organization has approved for installation and execution. This supports software

asset management by associating recognized applications with identifying details such as product name, publisher, version, or other inventory metadata. Such a list gives administrators a baseline for determining whether software observed on systems is sanctioned and can be managed according to organizational policy.

Maintaining this approved inventory is a core security practice because unmanaged applications can introduce unpatched vulnerabilities, unlicensed software, and unauthorized functionality. The CIS Controls emphasize actively managing enterprise assets and software so that the organization can identify authorized software and address software that is not approved. In operational terms, the displayed record is an allow-list or approved entry within the software-inventory process, rather than a report of patch status or a generic enumeration of every installed application on a particular endpoint.

See the CIS Critical Security Controls and CIS guidance on software inventory and control implementation.

QUESTION NO: 10

What is a recommended defense for the CIS Control for Application Software Security?

A. Keep debugging code in production web applications for quick troubleshooting

B. Limit access to the web application production environment to just the developers

C. Run a dedicated vulnerability scanner against backend databases

D. Display system error messages for only non-kernel related events

ANSWER: C

Explanation:

Run a dedicated vulnerability scanner against backend databases is the best answer because application software security requires regular, technically focused security testing to identify vulnerabilities before they can be exploited. Dedicated vulnerability-scanning tools can discover exposed services, weak configurations, known software flaws, insecure authentication settings, and other conditions that may affect the application's supporting data tier. Identifying such issues supports remediation and verification activities that are central to securing applications and the systems on which they rely.

CIS Controls guidance for Application Software Security emphasizes building security into the software lifecycle and validating applications through testing. In the current CIS Controls framework, this includes conducting application penetration testing and implementing security checks that help find security defects before release or during ongoing operation. Vulnerability scanning is a practical, repeatable defensive measure that contributes evidence for those validation efforts, particularly where the application interacts with backend infrastructure containing sensitive data. Scans should be authorized, appropriately scoped, performed routinely and after significant changes, and followed by documented remediation and retesting. See the CIS Critical Security Controls v8 and CIS's Application Software Security control guidance.

QUESTION NO: 11

What type of Unified Modelling Language (UML) diagram is used to show dependencies between logical groupings in a system?

A. Package diagram

B. Deployment diagram

C. Class diagram

D. Use case diagram

ANSWER: A

Explanation:

Package diagram is correct because it organizes UML model elements into packages, which are logical namespaces or groupings such as subsystems, layers, modules, or related classes. A package diagram can show the dependencies between these groupings, making it useful for expressing high-level architectural structure and the direction of coupling among parts of a system. For example, a presentation package may depend on an application-services package, which in turn depends on a domain package. This view helps architects and reviewers assess separation of concerns, layering, and the impact that changes in one logical area may have on another. UML defines Package as a namespace used to group named elements, and package diagrams commonly use dependency relationships between packages to represent these relationships at an abstraction level above individual classes. This directly matches the question's focus on dependencies between logical groupings rather than runtime infrastructure, individual data structures, or user interactions. See the Object Management Group's UML 2.5.1 specification and the UML package diagram reference for package and dependency notation details.