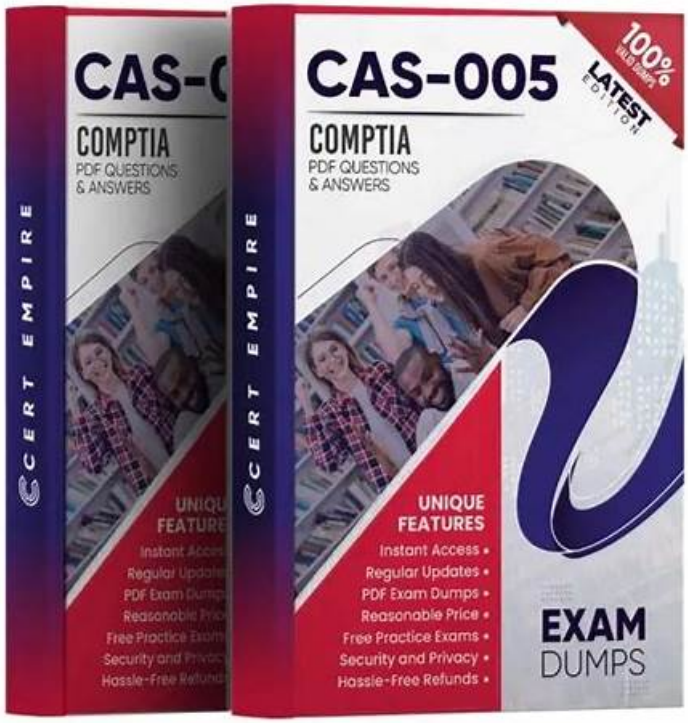
Actual CAS-005 Test Pdf & New CAS-005 Exam Format



P.S. Free 2025 CompTIA CAS-005 dumps are available on Google Drive shared by PDFDumps: https://drive.google.com/open?id=1LYiu_EQwRQsMGvCBBrmfc0r5-VuZY70K

The design of our CAS-005 guide training is ingenious and delicate. Every detail is perfect. For example, if you choose to study our CAS-005 learning materials on our windows software, you will find the interface our CAS-005 earning materials are concise and beautiful, so it can allow you to study CAS-005 Exam Questions in a concise and undisturbed environment. In addition, you will find a lot of small buttons, which can give you a lot of help. If you are satisfied with our CAS-005 exam questions, you can make a choice to purchase them.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering.
Topic 2	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
Topic 3	• Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems.
Topic 4	• Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security.

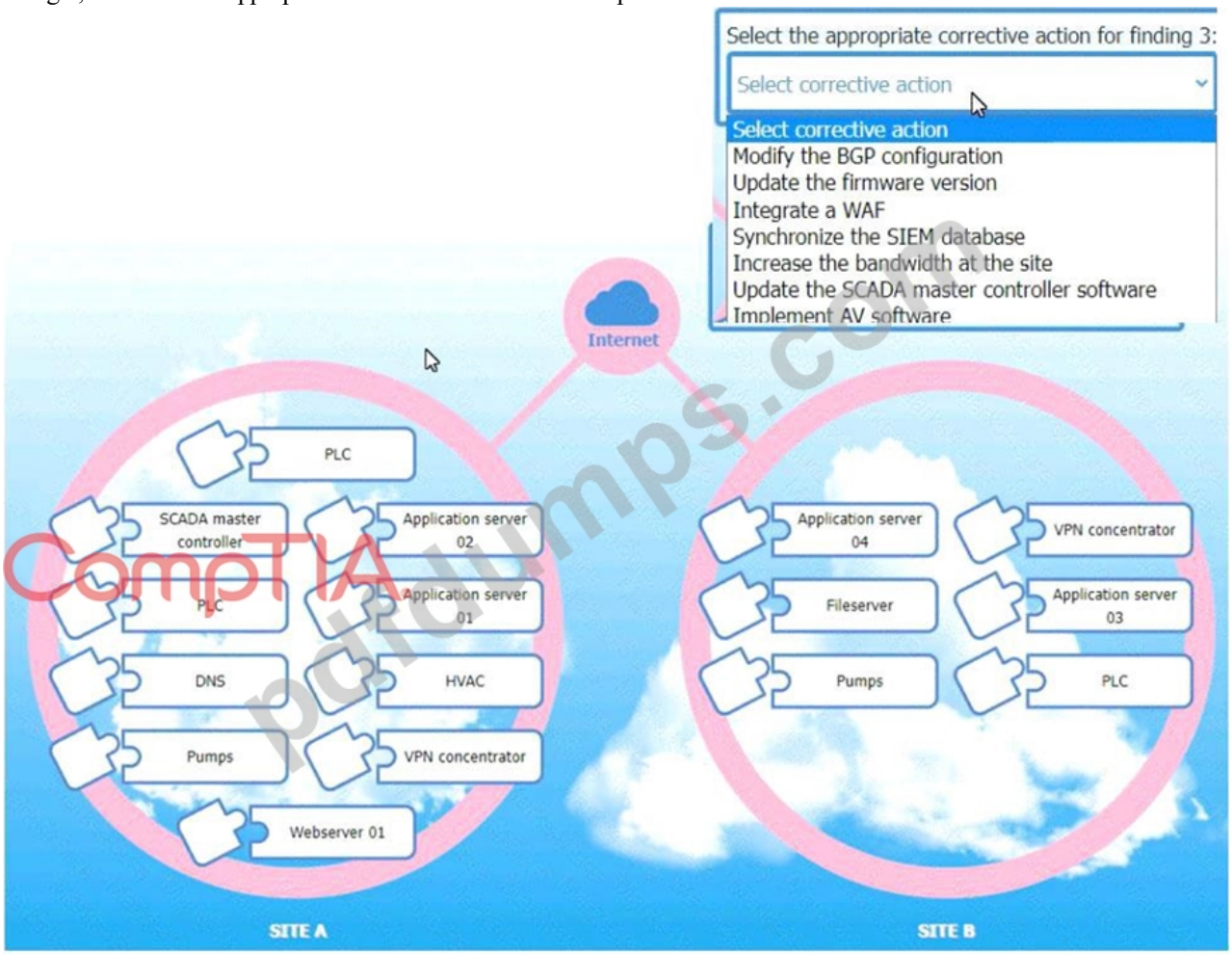
>> Actual CAS-005 Test Pdf <<

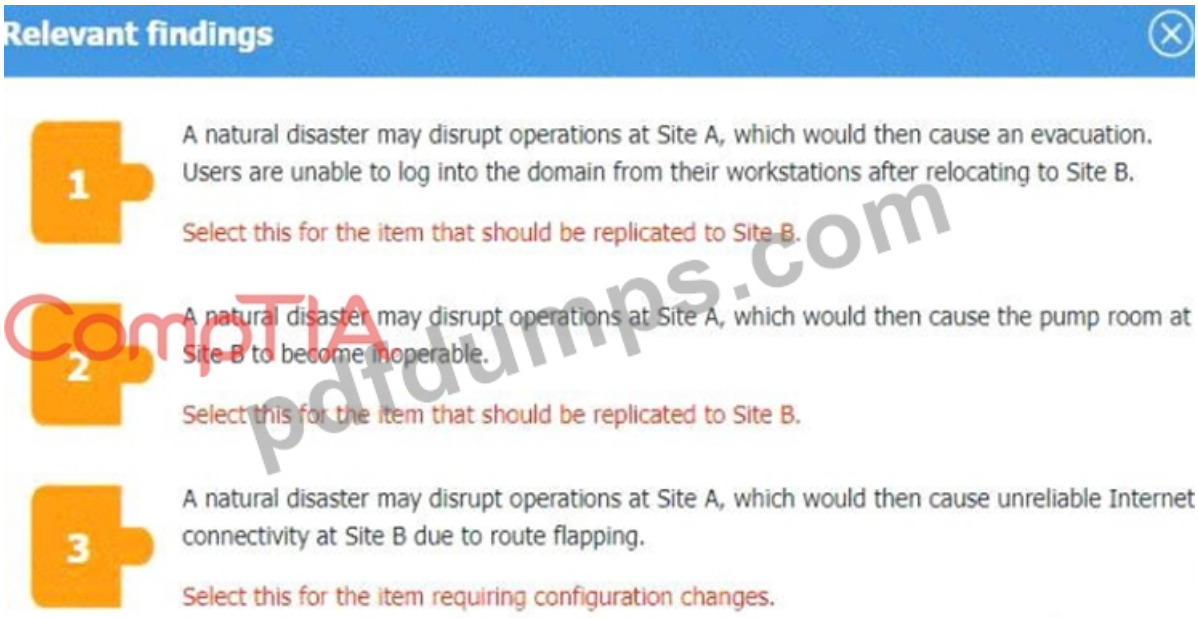
CAS-005 Practice Training - CAS-005 Free Download & CAS-005 Updated Torrent

In order to serve you better, we have a complete system for you. We offer you free demo for CAS-005 exam braindumps, and we recommend you have a try before buying. If you are quite satisfied with the free demo and want the complete version, you just need to add to cart and pay for it. You will receive the downloading link and password for CAS-005 Exam Dumps within ten minutes, if you don't receive, you can contact with us, and we will solve this problem for you. We offer you free update for one year for CAS-005 exam dumps after payment, so that you can obtain the latest information for the exam, and the latest information will be sent to you automatically.

CompTIA SecurityX Certification Exam Sample Questions (Q252-Q257):

NEW QUESTION # 252
An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:
1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from-their workstations after relocating to Site B.
2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.
INSTRUCTIONS
Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.
For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.





Answer:

Explanation:
See the complete solution below in Explanation:
Explanation:
Matching Relevant Findings to the Affected Hosts:
Finding 1:
Affected Host: DNS
Reason: Users are unable to log into the domain from their workstations after relocating to Site B, which implies a failure in domain name services that are critical for user authentication and domain login.
Finding 2:
Affected Host: Pumps
Reason: The pump room at Site B becoming inoperable directly points to the critical infrastructure components associated with pumping operations.
Finding 3:
Affected Host: VPN Concentrator
Reason: Unreliable internet connectivity at Site B due to route flapping indicates issues with network routing, which is often managed by VPN concentrators that handle site-to-site connectivity.
Corrective Actions for Finding 3:
Finding 3 Corrective Action:
Action: Modify the BGP configuration
Reason: Route flapping is often related to issues with Border Gateway Protocol (BGP) configurations.
Adjusting BGP settings can stabilize routes and improve internet connectivity reliability.
Replication to Site B for Finding 1:
Affected Host: DNS
Domain Name System (DNS) services are essential for translating domain names into IP addresses, allowing users to log into the network. Replicating DNS services ensures that even if Site A is disrupted, users at Site B can still authenticate and access necessary resources.
Replication to Site B for Finding 2:
Affected Host: Pumps
The operation of the pump room is crucial for maintaining various functions within the infrastructure.
Replicating the control systems and configurations for the pumps at Site B ensures that operations can continue smoothly even if Site A is affected.
Configuration Changes for Finding 3:
Affected Host: VPN Concentrator
Route flapping is a situation where routes become unstable, causing frequent changes in the best path for data to travel. This instability can be mitigated by modifying BGP configurations to ensure more stable routing.
VPN concentrators, which manage connections between sites, are typically configured with BGP for optimal routing.
References:
CompTIA Security+ Study Guide: This guide provides detailed information on disaster recovery and continuity of operations, emphasizing the importance of replicating critical services and making necessary configuration changes to ensure seamless operation

during disruptions.
CompTIA Security+ Exam Objectives: These objectives highlight key areas in disaster recovery planning, including the replication of critical services and network configuration adjustments.
Disaster Recovery and Business Continuity Planning (DRBCP): This resource outlines best practices for ensuring that operations can continue at an alternate site during a disaster, including the replication of essential services and network stability measures.
By ensuring that critical services like DNS and control systems for pumps are replicated at the alternate site, and by addressing network routing issues through proper BGP configuration, the organization can maintain operational continuity and minimize the impact of natural disasters on their operations.

NEW QUESTION # 253
A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

Date & Time	Public IP	Browser Info	Action
11 Dec 22:30:23	192.168.2.45	Mozilla/5.0 (Windows NT 5.1)	Access granted to admin
11 Dec 23:05:43	192.168.2.45	Mozilla/5.0 (Windows NT 5.1)	Access granted to admin
11 Dec 23:10:29	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Access granted to admin
11 Dec 23:12:18	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Logoff
12 Dec 00:05:43	104.18.16.29	Mozilla/5.0 (Linux x86_64)	Access granted to admin

Which of the following actions should the analyst take to best mitigate the threat?

- A. Upgrade the firmware on the camera.
- B. Block IP 104.18.16.29 on the firewall.
- C. Implement WAF protection for the web application.
- D. Only allowconnections from approved IPs.

Answer: D

Explanation:
The logs indicate unauthorized access from104.18.16.29, an external IP, to the building camera's administrative console during off-hours.Restricting access only to approved IPsensures that only authorized personnel can remotely control the cameras, reducing the risk of unauthorized access and manipulation.
* Implementing WAF protection (A)secures against web application attacks but does not restrict unauthorized administrative access.
* Upgrading the firmware (B)is good security hygiene but does not immediately mitigate the active threat.
* Blocking IP 104.18.16.29 (D)is a temporary measure, as an attacker can switch to another IP. A better long-term solution is whitelisting trusted IPs.
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 4.0 (Security Operations), Section onAccess Control and Network Security

NEW QUESTION # 254
A security analyst is reviewing the following authentication logs:

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

Which of the following should the analyst do first?

- A. Disable User12's account

- B. Disable User8's account
- C. Disable User1's account
- D. Disable User2's account

Answer: C

Explanation:
Based on the provided authentication logs, we observe that User1's account experienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12/15). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Here's a breakdown of why disabling User1's account is the appropriate first step:
* Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts:
* VM01 at 8:01:23 AM
* VM08 at 8:01:23 AM
* VM01 at 8:01:23 AM
* VM08 at 8:01:23 AM
* Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.
* Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further failed attempts, which might lead to successful unauthorized access if not addressed.
* References:
* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
* CompTIA Security+ Certification Exam Objectives
* NIST Special Publication 800-63B: Digital Identity Guidelines
By addressing User1's account first, we effectively mitigate the immediate threat of a brute-force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

NEW QUESTION # 255
Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:
* Full disk encryption
* Host-based firewall
* Time synchronization
* Password policies
* Application allow listing
* Zero Trust application access
Which of the following solutions best addresses the requirements? (Select two).

- A. HIDS
- B. SASE
- C. SBoM
- D. SCAP
- E. CASB

Answer: B,D

Explanation:
To address the specific OS benchmark configurations, the following solutions are most appropriate:
C: SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.
D: SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.
These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.
References:
CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.
NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

"Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth:
Covers the principles of Zero Trust and how SASE can implement them.
By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

NEW QUESTION # 256
A cloud engineer needs to identify appropriate solutions to:
* Provide secure access to internal and external cloud resources.
* Eliminate split-tunnel traffic flows.
* Enable identity and access management capabilities.
Which of the following solutions arc the most appropriate? (Select two).

- A. Microsegmentation
- B. SD-WAN
- C. CASB
- D. SASE
- E. PAM
- F. Federation

Answer: C,D

Explanation:
To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).
Why CASB and SASE?
* CASB (Cloud Access Security Broker):
* Secure Access: CASB solutions provide secure access to cloud resources by enforcing security policies and monitoring user activities.
* Identity and Access Management: CASBs integrate with identity and access management (IAM) systems to ensure that only authorized users can access cloud resources.
* Visibility and Control: They offer visibility into cloud application usage and control over data sharing and access.
* SASE (Secure Access Service Edge):
* Eliminate Split-Tunnel Traffic: SASE integrates network security functions with WAN capabilities to ensure secure access without the need for split-tunnel configurations.
* Comprehensive Security: SASE provides a holistic security approach, including secure web gateways, firewalls, and zero trust network access (ZTNA).
* Identity-Based Access: SASE leverages IAM to enforce access controls based on user identity and context.
Other options, while useful, do not comprehensively address all the requirements:
* A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.
* B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.
* D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.
* E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.
References:
* CompTIA SecurityX Study Guide
* "CASB: Cloud Access Security Broker," Gartner Research

NEW QUESTION # 257
.....

- High-quality Actual CAS-005 Test Pdf - Useful New CAS-005 Exam Format Ensure You a High Passing Rate □ The page for free download of ☀ CAS-005 □☀□ on ▹ www.pdfdumps.com ◃ will open immediately □Exam CAS-005 Questions
- CompTIA CAS-005 Practice Test Learning Material in Three Different Formats □ Copy URL （ www.pdfvce.com ） open and search for （ CAS-005 ） to download for free □Certified CAS-005 Questions
- Exam CAS-005 Vce □ Latest CAS-005 Dumps Pdf □ New CAS-005 Test Topics □ Download ▹ CAS-005 ◃ for free by simply searching on ⇛ www.passtestking.com ⇚ □CAS-005 Reliable Source
- CAS-005 Valid Test Pattern 🈵 CAS-005 Test Papers □ CAS-005 Practice Exam Online □ Search for ▸ CAS-005 ◂ on ⇛ www.pdfvce.com ⇚ immediately to obtain a free download □CAS-005 Reliable Exam Materials
- CAS-005 Guide Torrent and CAS-005 Study Tool - CAS-005 Exam Torrent ✈ Search for [CAS-005] and download exam materials for free through ➠ www.prep4away.com □ □Latest CAS-005 Dumps Pdf
- CAS-005 Pass Torrent - CAS-005 Exam Guide - CAS-005 Exam Pass4Sure □ Search for ➠ CAS-005 □ and download it for free on ➤ www.pdfvce.com □ website □Latest CAS-005 Dumps Pdf
- CAS-005 Exams Training □ CAS-005 Exam Review □ CAS-005 Test Papers □ Search for ➤ CAS-005 □ and download it for free on ➠ www.pdfdumps.com □ website □CAS-005 Valid Test Pattern
- High-quality Actual CAS-005 Test Pdf - Useful New CAS-005 Exam Format Ensure You a High Passing Rate □ Open website ➽ www.pdfvce.com □ and search for ➽ CAS-005 □ for free download □CAS-005 Exam Review
- CAS-005 Exams Training □ CAS-005 Reliable Exam Sims □ Exam CAS-005 Vce □ Open ➠ www.pass4test.com □ □ and search for 【 CAS-005 】 to download exam materials for free □Exam CAS-005 Questions
- CompTIA CAS-005 Dumps [2025] - To Acquire Very Best Final Results □ □ www.pdfvce.com □ is best website to obtain { CAS-005 } for free download □New CAS-005 Test Topics
- CompTIA CAS-005 Dumps [2025] - To Acquire Very Best Final Results □ Search for { CAS-005 } and download it for free on “ www.examsreviews.com ” website □CAS-005 Reliable Exam Sims
- startingedu.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, ncon.edu.sa, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, farmasidemy.com, daotao.wisebusiness.edu.vn, motionentrance.edu.np, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, almasar.org, Disposable vapes

P.S. Free 2025 CompTIA CAS-005 dumps are available on Google Drive shared by PDFDumps: https://drive.google.com/open?id=1LYiu_EQwRQsMGvCBBrmfc0r5-VuZY70K