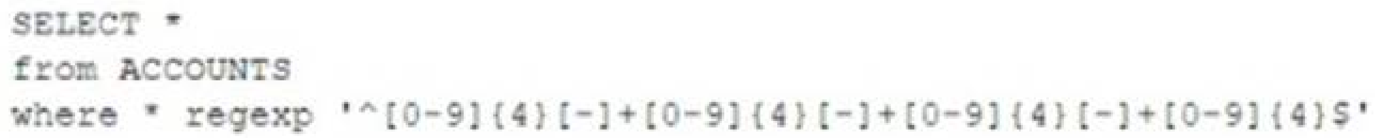
CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the Jogs. the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:



```
SELECT *
from ACCOUNTS
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

Assuming this query was used to acquire and exfiltrate data, which of the following types of
data was compromised, and what steps should the incident response plan contain?
A) Personal health information: Inform the human resources department of the breach and review the DLP logs.
) Account history; Inform the relationship managers of the breach and create new accounts for the affected users.
C) Customer IDs: Inform the customer service department of the breach and work to change the account numbers.
D) PAN: Inform the legal department of the breach and look for this data in dark web monitoring.

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 2
A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated Oss. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

A. Segment the systems to reduce the attack surface if an attack occurs
B. Migrate the services to new systems with a supported and patched OS.
C. Patch the systems to the latest versions of the existing OSs
D. Install anti-malwar
E. HIPS, and host-based firewalls on each of the systems

Answer: B

NEW QUESTION 3
An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization’s headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:
Low latency for all mobile users to improve the users’ experience SSL offloading to improve web server performance
Protection against DoS and DDoS attacks High availability
Which of the following should the organization implement to BEST ensure all requirements are met?

A. A cache server farm in its datacenter
B. A load-balanced group of reverse proxy servers with SSL acceleration
C. A CDN with the origin set to its datacenter
D. Dual gigabit-speed Internet connections with managed DDoS prevention

Answer: B

NEW QUESTION 4
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

A. Remote provider BCDR
B. Cloud provider BCDR
C. Alternative provider BCDR
D. Primary provider BCDR

Answer: B

NEW QUESTION 5
A company’s employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation? (Select TWO.)

A. Outdated escalation attack
B. Privilege escalation attack
C. VPN on the mobile device
D. Unrestricted email administrator accounts
E. Chief use of UDP protocols
F. Disabled GPS on mobile devices

Answer: CF

NEW QUESTION 6

An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:
• Some developers can directly publish code to the production environment.
• Static code reviews are performed adequately.
• Vulnerability scanning occurs on a regularly scheduled basis per policy.
Which of the following should be noted as a recommendation within the audit report?

A. Implement short maintenance windows.
B. Perform periodic account reviews.
C. Implement job rotation.
D. Improve separation of duties.

Answer: D

NEW QUESTION 7
An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently,
the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.
Which of the following designs would be BEST for the CISO to use?

A. Adding a second redundant layer of alternate vendor VPN concentrators
B. Using Base64 encoding within the existing site-to-site VPN connections
C. Distributing security resources across VPN sites
D. Implementing IDS services with each VPN concentrator
E. Transitioning to a container-based architecture for site-based services

Answer: A

Explanation:
If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

NEW QUESTION 8
A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.
Which of the following techniques would BEST support this?

A. Configuring systemd services to run automatically at startup
B. Creating a backdoor
C. Exploiting an arbitrary code execution exploit
D. Moving laterally to a more authoritative server/service

Answer: B

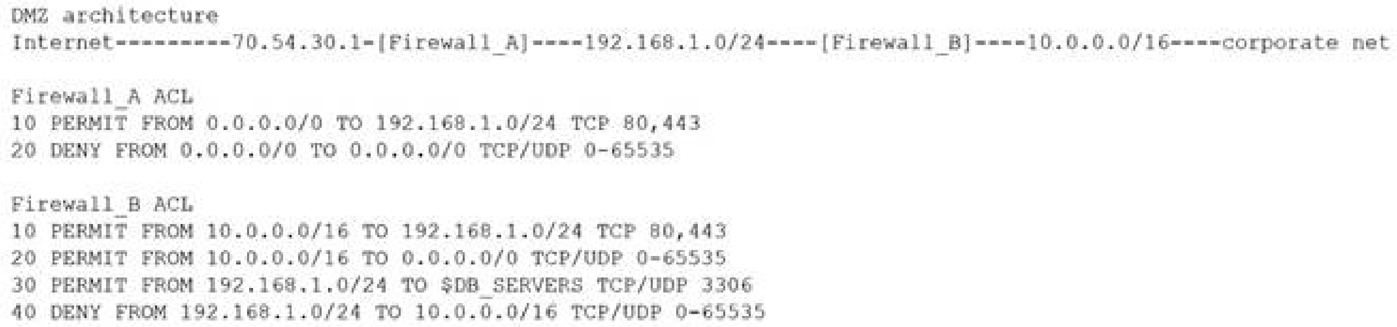
NEW QUESTION 9
A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

A. DLP
B. Mail gateway
C. Data flow enforcement
D. UTM

Answer: A

Explanation:
A DLP system is the best option for the company to mitigate the risk of losing its proprietary enhancements to competitors. DLP stands for data loss prevention, which is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block data transfers based on predefined rules and criteria, such as content, source, destination, etc. DLP can help protect the company's intellectual property and trade secrets from being compromised by malicious actors or accidental leaks. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how- does-it-work.html

NEW QUESTION 10
A security architect is reviewing the following proposed corporate firewall architecture and configuration:



```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

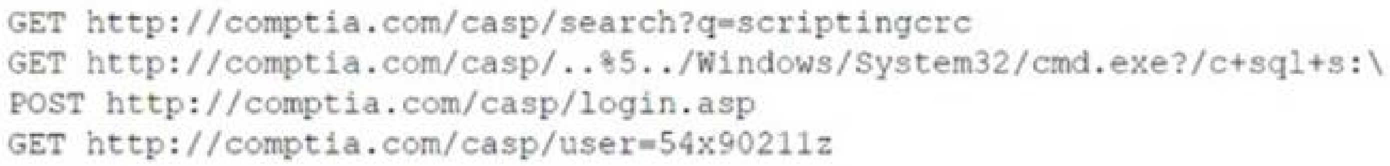
Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
Web servers must receive all updates via HTTP/S from the corporate network. Web servers should not initiate communication with the Internet.
Web servers should only connect to preapproved corporate database servers.
Employees' computing devices should only connect to web services over ports 80 and 443. Which of the following should the architect recommend to ensure all

requirements are met
in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP80,443
C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0- 65535
F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Answer: AD

NEW QUESTION 10
A security analyst needs to recommend a remediation to the following threat:



```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

A. Patch the system.
B. Update the antivirus.
C. Install a host-based firewall.
D. Enable TLS 1.2.

Answer: D

NEW QUESTION 15
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line.
Which of the following commands would be the BEST to run to view only active Internet connections?

A. sudo netstat -antu | grep “LISTEN” | awk ‘{print$5}’
B. sudo netstat -nlt -p | grep “ESTABLISHED”
C. sudo netstat -plntu | grep -v “Foreign Address”
D. sudo netstat -pnut -w | column -t -s $’\w’
E. sudo netstat -pnut | grep -P ^tcp

Answer: E

Explanation:
Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port
The netstat command is a tool that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The command has various options that can modify its output. The options used in the correct answer are:
p: Show the PID and name of the program to which each socket belongs.
n: Show numerical addresses instead of trying to determine symbolic host, port or user names.
u: Show only UDP connections. t: Show only TCP connections.
The grep command is a tool that searches for a pattern in a file or input. The option used in the correct answer is:
P: Interpret the pattern as a Perl-compatible regular expression (PCRE).
The pattern used in the correct answer is ^tcp, which means any line that starts with tcp. This will filter out any UDP connections from the output.
The sudo command is a tool that allows a user to run programs with the security privileges of another user (usually the superuser or root). This is necessary to run the netstat command with the -p option, which requires root privileges.
The correct answer will show only active TCP connections with numerical addresses and program names, which can be considered as active Internet connections. The other answers will either show different types of connections (such as listening or local), use different options that are not relevant (such as -a, -l, -w, or -s), or use different commands that are not useful (such as awk or column). References: https://man7.org/linux/man- pages/man8/netstat.8.html https://man7.org/linux/man-pages/man1/grep.1.html https://man7.org/linux/man-pages/man8/sudo.8.html

NEW QUESTION 19
A company just released a new video card. Due to limited supply and nigh demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's Intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

A. Inherent Low
B. Mitigated
C. Residual
D. Transferred

Answer: A

NEW QUESTION 24
A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.
This is an example of:

A. due intelligence
B. e-discovery.
C. due care.

D. legal hold.

Answer: A

Explanation:
Reference: https://www.ansarada.com/due-diligence/hr

NEW QUESTION 29
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

A. NX bit
B. ASLR
C. DEP
D. HSM

Answer: B

Explanation:
https://eklitzke.org/memory-protection-and-aslr
ASLR (Address Space Layout Randomization) is a technology that can mitigate the manipulation of memory segments caused by a buffer overflow attack. ASLR randomizes the location of memory segments, such as the stack, heap, or libraries, making it harder for an attacker to predict or control where to inject malicious code or overwrite memory segments. NX bit (No-eXecute bit) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. NX bit marks certain memory segments as non-executable, preventing an attacker from running code in those segments. DEP (Data Execution Prevention) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. DEP uses hardware and software mechanisms to mark certain memory regions as data-only, preventing an attacker from running code in those regions. HSM (Hardware Security Module) is a device that can provide cryptographic functions and key storage, but it does not mitigate the manipulation of memory segments
caused by a buffer overflow attack. Verified References: https://www.comptia.org/blog/what-is-aslr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 34
An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API. Given this information, which of the following is a noted risk?

A. Feature delay due to extended software development cycles
B. Financial liability from a vendor data breach
C. Technical impact to the API configuration
D. The possibility of the vendor's business ceasing operations

Answer: A

Explanation:
Reference: https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability

NEW QUESTION 37
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5
B. 8
C. 50
D. 36,500

Answer: A

Explanation:
Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative- risk-analysis/
The ARO (annualized rate of occurrence) for successful breaches is the number of times an event is expected to occur in a year. To calculate the ARO for successful breaches, the engineer can divide the number of breaches by the number of years. In this case, the company's data has been breached two times in four years, so the ARO is 2 / 4 = 0.5. The other options are incorrect calculations. Verified References: https://www.comptia.org/blog/what-is-risk-management https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 39
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

A. Cookies
B. Wildcard certificates
C. HSTS
D. Certificate pinning

Answer: D

Explanation:

Reference: https://cloud.google.com/security/encryption-in-transit
Certificate pinning is a technique that can prevent HTTPS interception attacks by hardcoding the expected certificate or public key of the server in the application code, so that any certificate presented by an intermediary will be rejected. Cookies are small pieces of data that are stored by browsers to remember user preferences or sessions, but they do not prevent HTTPS interception attacks. Wildcard certificates are certificates that can be used for multiple subdomains of a domain, but they do not prevent HTTPS interception attacks. HSTS (HTTP Strict Transport Security) is a policy that forces browsers to use HTTPS connections, but it does not prevent HTTPS interception attacks. Verified References: https://www.comptia.org/blog/what-is-certificate-pinning
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 44
A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:
22
25
110
137
138
139
445
Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.
B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Answer: A

NEW QUESTION 49
An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

A. SDLC attack
B. Side-load attack
C. Remote code signing
D. Supply chain attack

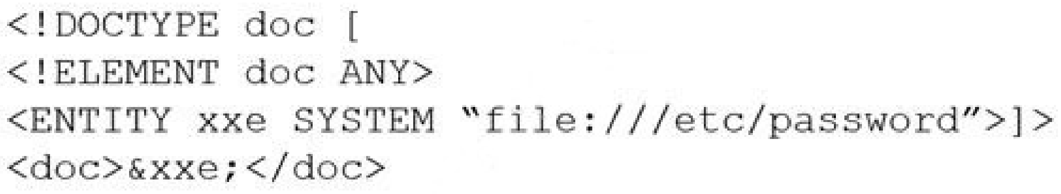
Answer: D

NEW QUESTION 53
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory OPOs
B. PKI certificates
C. Host-based firewall
D. NAC persistent agent

Answer: B

NEW QUESTION 56
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:



```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<ENTITY xxe SYSTEM "file:///etc/password">]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

A. CAPTCHA
B. Input validation
C. Data encoding
D. Network intrusion prevention

Answer: B

Explanation:
Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

NEW QUESTION 60
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

A. E-discovery
B. Review analysis

C. Information governance
D. Chain of custody

Answer: A

Explanation:
E-discovery is the process of searching and collecting evidence during an investigation or lawsuit. E-discovery involves identifying, preserving, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant for a legal case or investigation. E-discovery can be used to find evidence in email, business communications, social media, online documents, databases, and other digital sources. The other options are either irrelevant or less effective for the given scenario

NEW QUESTION 62
A help desk technician just informed the security department that a user downloaded a suspicious file from internet explorer last night. The user confirmed accessing all the files and folders before going home from work. the next morning, the user was no longer able to boot the system and was presented a screen with a phone number. The technician then
tries to boot the computer using wake-on-LAN, but the system would not come up. which of the following explains why the computer would not boot?

A. The operating system was corrupted.
B. SElinux was in enforced status.
C. A secure boot violation occurred.
D. The disk was encrypted.

Answer: A

NEW QUESTION 64
A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce
• Cloud-delivered services
• Full network security stack
• SaaS application security management
• Minimal latency for an optimal user experience
• Integration with the cloud 1AM platform Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)
B. NGFW
C. Managed Security Service Provider (MSSP)
D. SASE

Answer: D

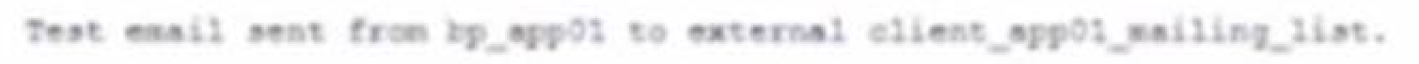
NEW QUESTION 67
Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the security administrator notices the human resources department is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

A. Modify the ACLS.
B. Review the Active Directory.
C. Update the marketing department's browser.
D. Reconfigure the WAF.

Answer: A

Explanation:
Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud application or its data sources. The other options are either irrelevant or less effective for the given scenario.

NEW QUESTION 71
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.



```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

Explanation:
The best option for the security analyst to perform is to contact the security department at the business partner and alert them to the email event. The email appears to be a phishing attempt that tries to trick the employees into revealing their login credentials by impersonating a legitimate sender. The security department at the business partner should be notified so they can investigate the source and scope of the attack and take appropriate actions to protect their systems and users. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://us-cert.cisa.gov/ncas/tips/ST04-014

NEW QUESTION 76
A software development company is building a new mobile application for its social media platform. The company wants to gain its Users' rust by reducing the risk of on-path attacks between the mobile client and its servers and
by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status.
* Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Answer: BF

Explanation:
OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the
social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks.

NEW QUESTION 79
A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?

A. TPM
B. HSM
C. PKI
D. UEFI/BIOS

Answer: A

Explanation:
A TPM (trusted platform module) is a hardware device that can provide boot
loader protection by storing cryptographic keys and verifying the integrity of the boot process. An HSM (hardware security module) is similar to a TPM, but it is used for storing keys for applications, not for booting. A PKI (public key infrastructure) is a system of certificates and keys that can provide encryption and authentication, but not boot loader protection. UEFI/BIOS are firmware interfaces that control the boot process, but they do not provide protection by themselves. Verified References: https://www.comptia.org/blog/what- is-a-tpm-trusted-platform-module https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 81
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency
B. Data exposure
C. Data loss
D. Data dispersion

Answer: B

Explanation:
Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified References: https://www.comptia.org/blog/what-is-data-exposure
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 85
An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:
* Be based on open-source Android for user familiarity and ease.
* Provide a single application for inventory management of physical assets.
* Permit use of the camera be only the inventory application for the purposes of scanning
* Disallow any and all configuration baseline modifications.
* Restrict all access to any device resource other than those requirement ?

A. Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.
B. Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
C. Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
D. Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

Answer: A

NEW QUESTION 87

SIMULATION

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

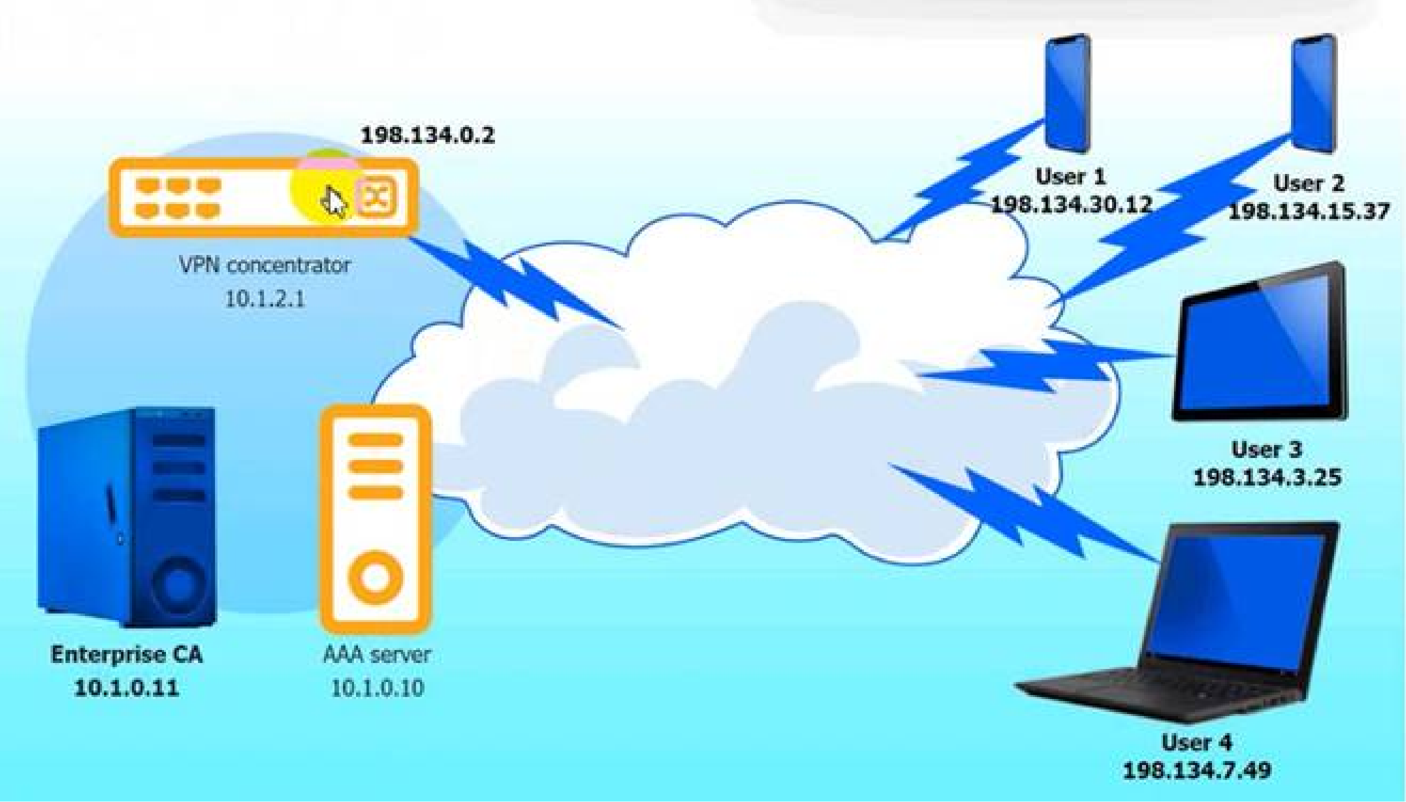
Complete the configuration files to meet the following requirements:

- The EAP method must use mutual certificate-based authentication (With issued client certificates).
- The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
- The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

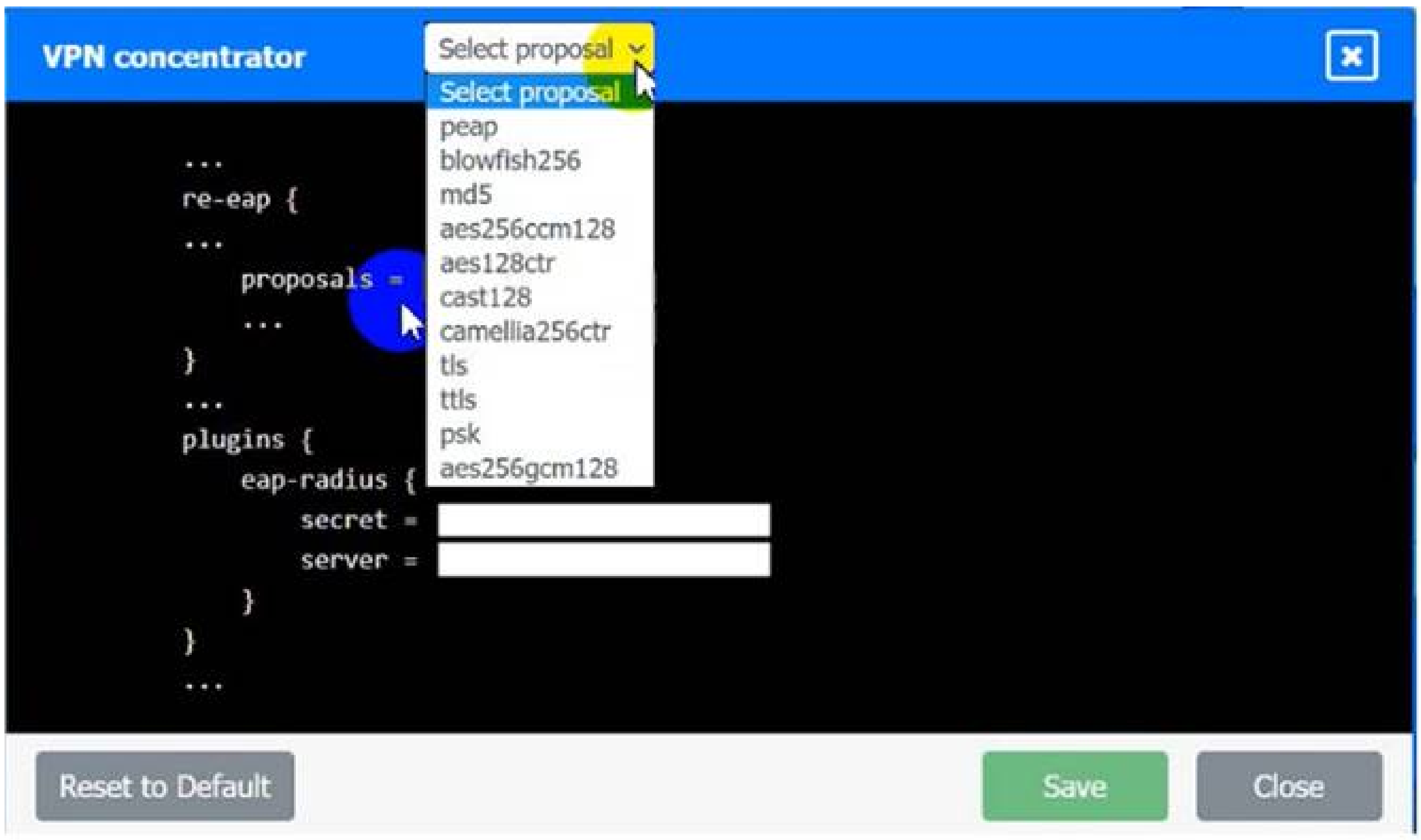
INSTRUCTIONS

Click on the AAA server and VPN concentrator to complete the configuration.

Fill in the appropriate fields and make selections from the drop-down menus.

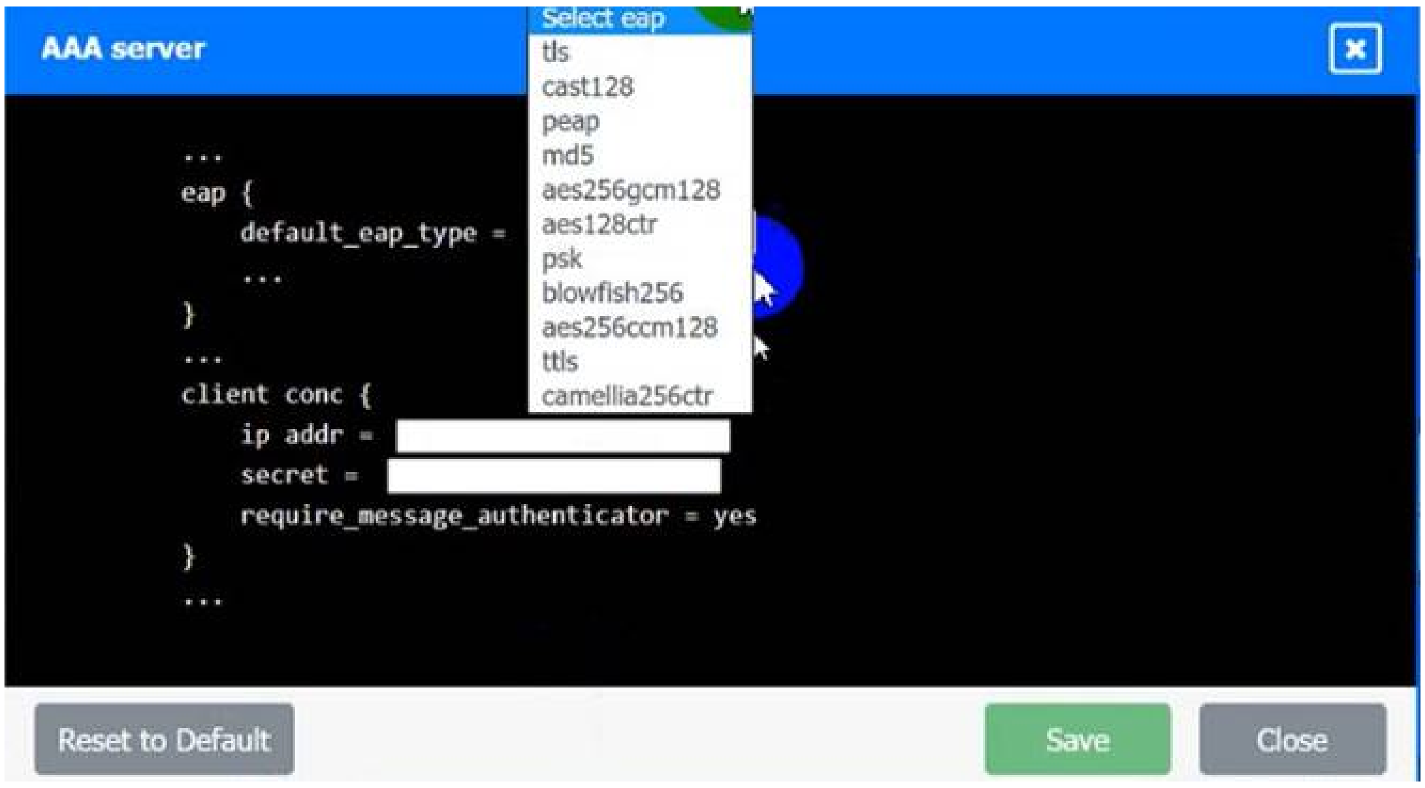


VPN Concentrator:



```
    ...
    re-eap {
    ...
        proposals =
        ...
    }
    ...
    plugins {
        eap-radius {
            secret =
            server =
        }
    }
    ...
```

AAA Server:

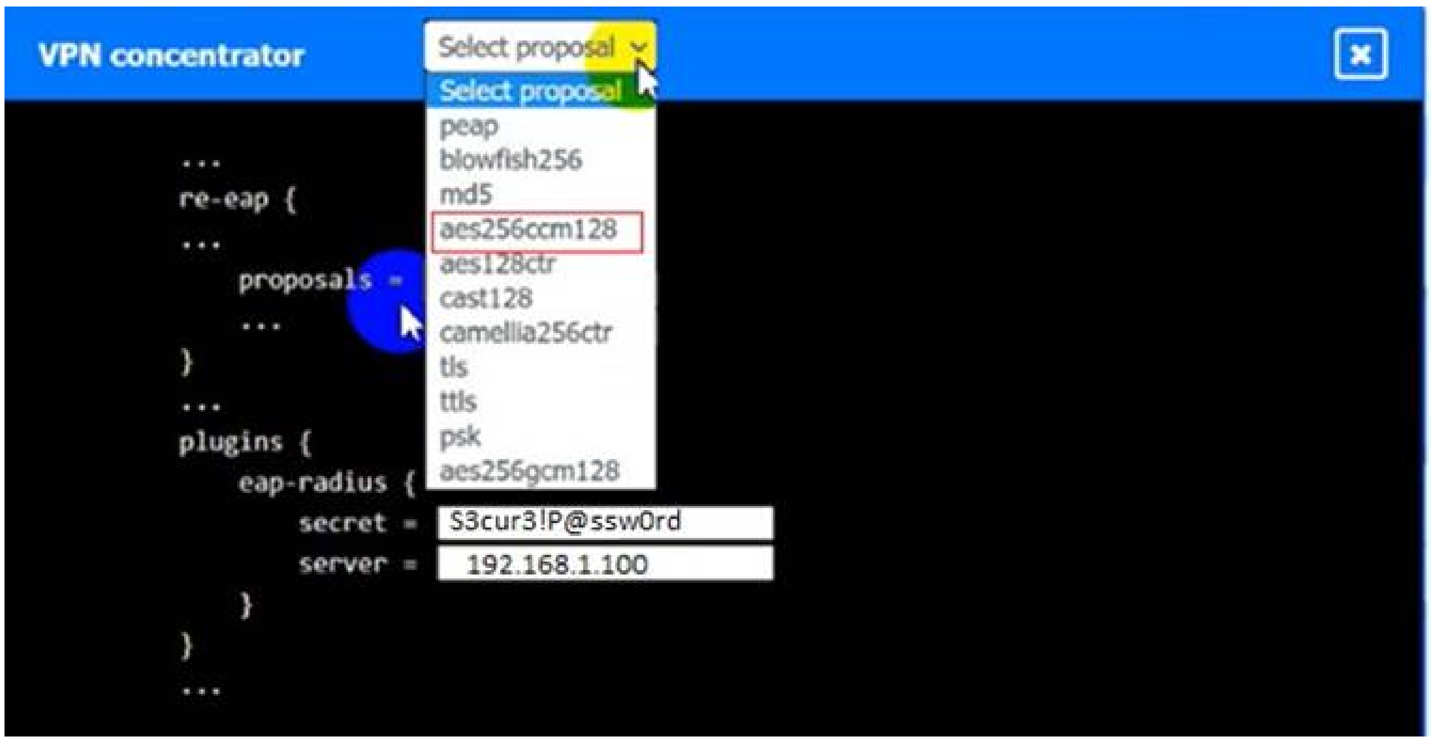


```
...
eap {
    default_eap_type =
    ...
}
...
client conc {
    ip addr =
    secret =
    require_message_authenticator = yes
}
...
```

A. Mastered
B. Not Mastered

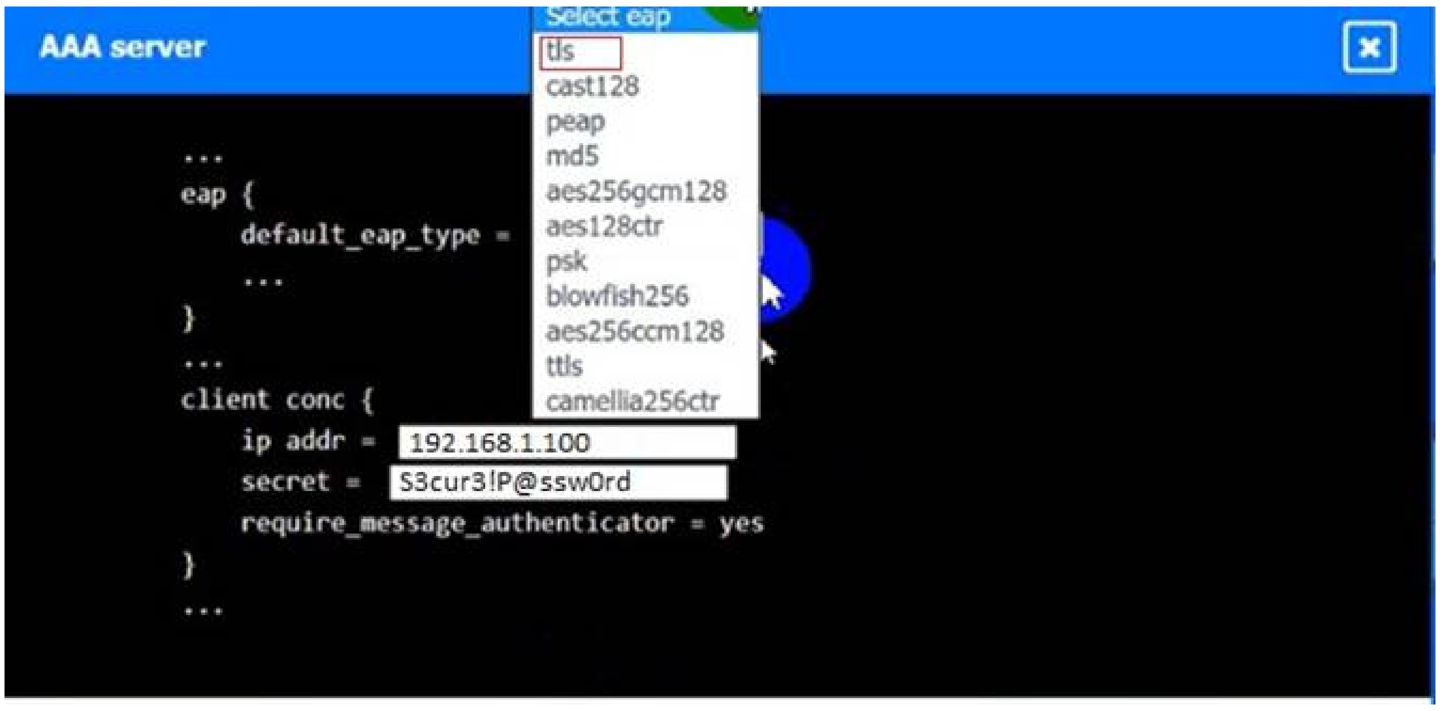
Answer: A

Explanation:
VPN Concentrator:



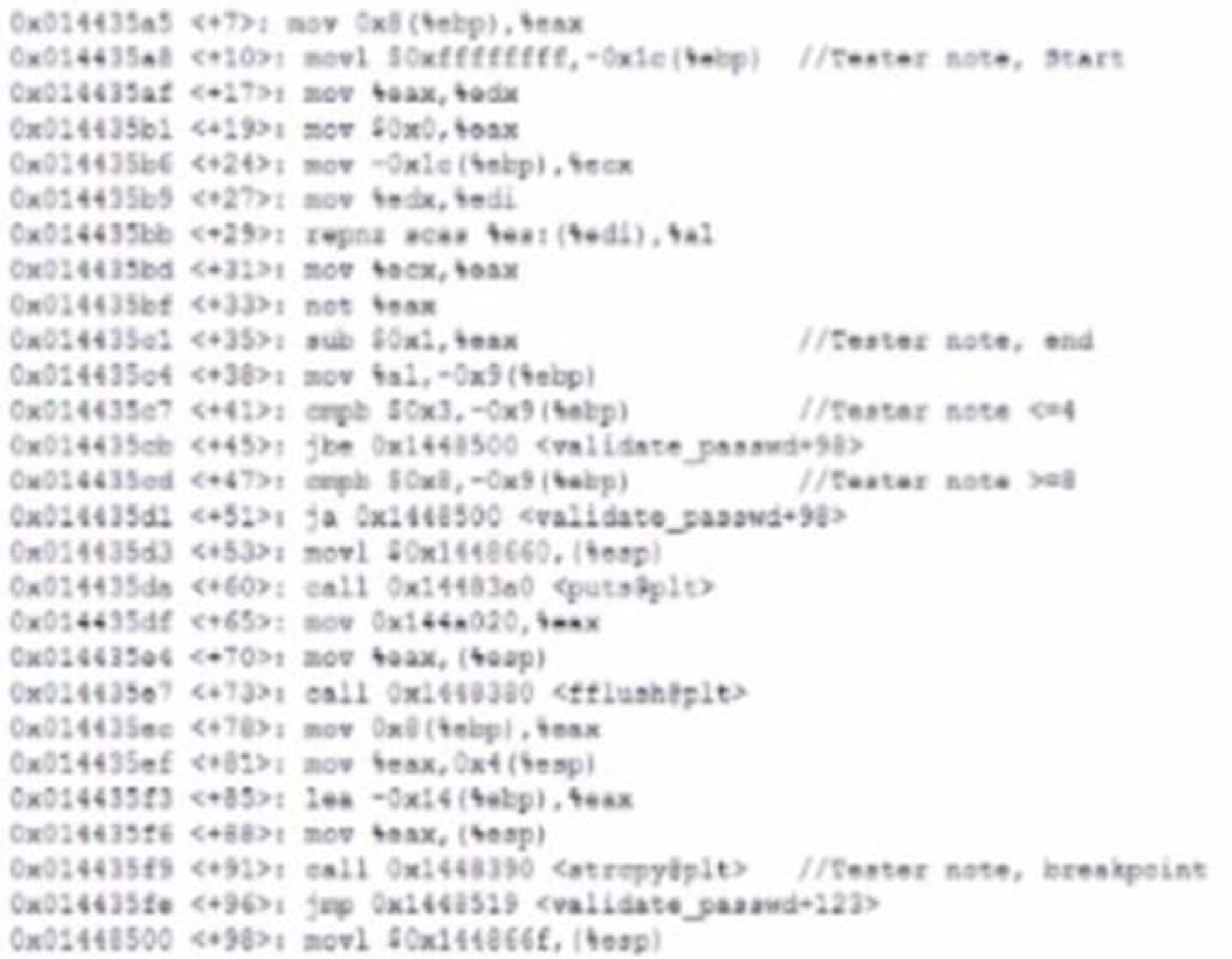
```
...
re-eap {
...
    proposals =
    ...
}
...
plugins {
    eap-radius {
        secret = S3cur3!P@ssw0rd
        server = 192.168.1.100
    }
}
...
```

AAA Server:



```
...
eap {
    default_eap_type =
    ...
}
...
client conc {
    ip addr = 192.168.1.100
    secret = S3cur3!P@ssw0rd
    require_message_authenticator = yes
}
...
```

NEW QUESTION 88
A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:



```
0x014435a5 <+7>: mov 0x8(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp)   //Tester note, Start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov $0x0,%eax
0x014435b6 <+24>: mov -0x1c(%ebp),%ecx
0x014435b9 <+27>: mov %edx,%edi
0x014435bb <+29>: repnz scas %es:(%edi),%al
0x014435bd <+31>: mov %ecx,%eax
0x014435bf <+33>: not %eax
0x014435c1 <+35>: sub $0x1,%eax                  //Tester note, end
0x014435c4 <+38>: mov %al,-0x9(%ebp)
0x014435c7 <+41>: cmpb $0x3,-0x9(%ebp)           //Tester note <=4
0x014435cb <+45>: jbe 0x1448500 <validate_passwd+98>
0x014435cd <+47>: cmpb $0x8,-0x9(%ebp)           //Tester note >=8
0x014435d1 <+51>: ja 0x1448500 <validate_passwd+98>
0x014435d3 <+53>: movl $0x1448660,(%esp)
0x014435da <+60>: call 0x14483a0 <puts@plt>
0x014435df <+65>: mov 0x144a020,%eax
0x014435e4 <+70>: mov %eax,(%esp)
0x014435e7 <+73>: call 0x1448380 <fflush@plt>
0x014435ec <+78>: mov 0x8(%ebp),%eax
0x014435ef <+81>: mov %eax,0x4(%esp)
0x014435f3 <+85>: lea -0x14(%ebp),%eax
0x014435f6 <+88>: mov %eax,(%esp)
0x014435f9 <+91>: call 0x1448390 <strcpy@plt>   //Tester note, breakpoint
0x014435fe <+96>: jmp 0x1448519 <validate_passwd+123>
0x01448500 <+98>: movl $0x144866f,(%esp)
```

The penetration testers MOST likely took advantage of:

A. A TOC/TOU vulnerability
B. A plain-text password disclosure
C. An integer overflow vulnerability
D. A buffer overflow vulnerability

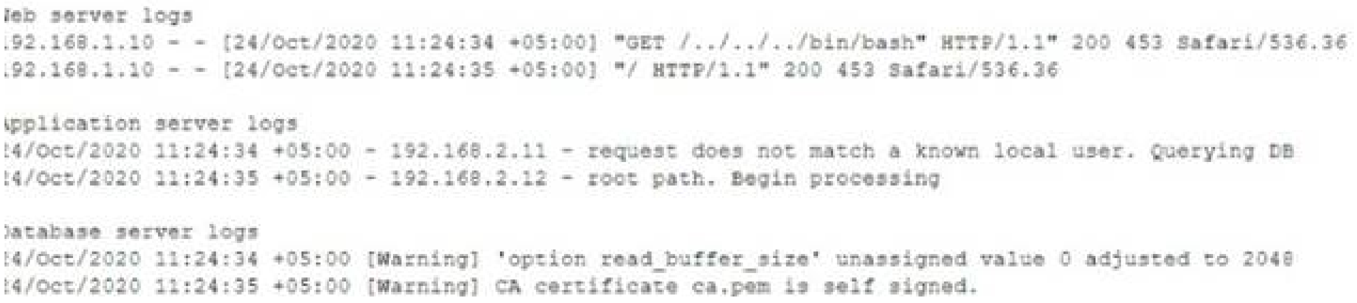
Answer: A

NEW QUESTION 89
An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately. many Of the applications are provided only as compiled binaries. Which Of the following should the organization use to analyze these applications? (Select TWO).

A. Regression testing
B. SAST
C. Third-party dependency management
D. IDE SAST
E. Fuzz testing
F. IAST

Answer: DE

NEW QUESTION 91
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:



```
Web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200 453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

A. Enable the x-Forwarded-For header al the load balancer.
B. Install a software-based HIDS on the application servers.
C. Install a certificate signed by a trusted CA.
D. Use stored procedures on the database server.
E. Store the value of the $_server (' REMOTE_ADDR '] received by the web servers.

Answer: C

NEW QUESTION 95
An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.

Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

A. NIST
B. GDPR
C. PCI DSS
D. ISO

Answer: C

Explanation:
PCI DSS (Payment Card Industry Data Security Standard) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a standard that provides the best guidance for protecting credit card information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified References: https://www.comptia.org/blog/what-is-pci-dss https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 96
An organization is implementing a new identity and access management architecture with the following objectives:
Supporting MFA against on-premises infrastructure
Improving the user experience by integrating with SaaS applications Applying risk-based policies based on location
Performing just-in-time provisioning
Which of the following authentication protocols should the organization implement to support these requirements?

A. Kerberos and TACACS
B. SAML and RADIUS
C. OAuth and OpenID
D. OTP and 802.1X

Answer: C

Explanation:
Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate- application-authentication-to-azure-active-directory
OAuth and OpenID are two authentication protocols that can support the objectives of the organization. OAuth is a protocol that allows users to grant access to their resources on one site (or service) to another site (or service) without sharing their credentials. OpenID is a protocol that allows users to use an existing account to sign in to multiple websites without creating new passwords. Both protocols can support MFA, SaaS integration, risk- based policies, and just-in-time provisioning. References: https://auth0.com/docs/protocols/oauth2 https://openid.net/connect/

NEW QUESTION 101
A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client's systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
B. The change control board must review and approve a submission.
C. The information system security officer provides the systems engineer with the system updates.
D. The security engineer asks the project manager to review the updates for the client's system.

Answer: B

Explanation:
The change control board (CCB) is a committee that consists of subject matter experts and managers who decide whether to implement proposed changes to a project. The change control board is part of the change management plan, which defines the roles and processes for managing change within a team or organization. The change control board must review and approve a submission for any change request that affects the scope, schedule, budget, quality, or risks of the project. The change control board evaluates the impact and benefits of the change request and decides whether to accept, reject, or defer it.
* A. The implementation engineer requesting direct approval from the systems engineer and the Chief Information Security Officer is not a correct process for requesting updates or corrections to the client’s systems, because it bypasses the change control board and the project manager. This could lead to unauthorized changes that could compromise the project’s objectives and deliverables.
* C. The information system security officer providing the systems engineer with the system updates is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board or the project manager. This could lead to unauthorized changes that could introduce security vulnerabilities or conflicts with other system components.
* D. The security engineer asking the project manager to review the updates for the client’s system is not a correct process for requesting updates or corrections to the client’s systems, because it does not involve the change control board. The project manager is
responsible for facilitating the change management process, but not for approving or rejecting change requests.
https://www.projectmanager.com/blog/change-control-board-roles-responsibilities- processes

NEW QUESTION 104
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: B

Explanation:
PAM (Privileged Access Management) is a solution that can increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. By implementing PAM, removing users from the local administrators group, and prompting users for explicit approval when elevated privileges are required, the security engineer can reduce the attack surface, prevent unauthorized access, and enforce the principle of least privilege. Implementing PAM, keeping users in the local administrators group, and enabling local administrator account monitoring may not provide enough control or visibility over local administrator accounts, as users could still abuse or compromise their privileges. Implementing EDR (Endpoint Detection and Response) may not provide enough control or visibility over local administrator accounts, as EDR is mainly focused on detecting and responding to threats, not managing privileges. Enabling user behavior analytics may not provide enough control or visibility over local administrator accounts, as user behavior analytics is mainly focused on identifying anomalies or risks in user activity, not managing privileges. Verified References: https://www.comptia.org/blog/what-is-pam https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 108
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A. Pay the ransom within 48 hours.
B. Isolate the servers to prevent the spread.
C. Notify law enforcement.
D. Request that the affected servers be restored immediately.

Answer: B

Explanation:
Isolating the servers is the best immediate action to take after reporting the incident to the management team, as it can limit the damage and contain the ransomware infection. Paying the ransom is not advisable, as it does not guarantee the recovery of the data and may encourage further attacks. Notifying law enforcement is a possible step, but not the next one after reporting. Requesting that the affected servers be restored immediately may not be feasible or effective, as it depends on the availability and integrity of backups, and it does not address the root cause of the attack. Verified References: https://www.comptia.org/blog/what-is-ransomware-and-how-to-protect-yourself https://www.comptia.org/certifications/comptia-advanced-security-practitioner

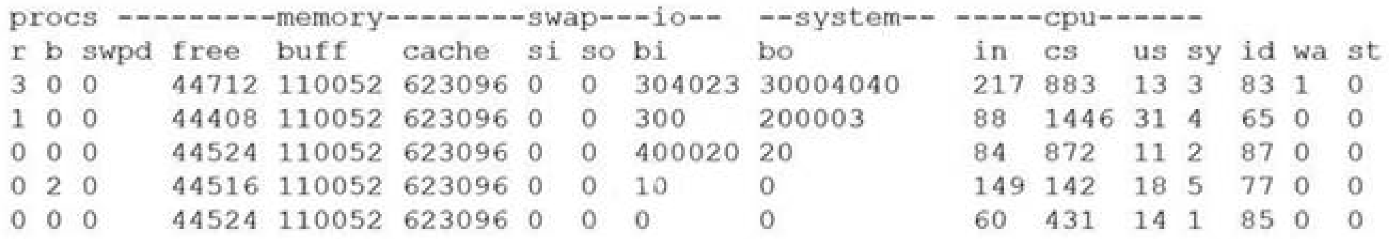
NEW QUESTION 111
A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.
Which of the following would be BEST for the company to implement?

A. A WAF
B. An IDS
C. A SIEM
D. A honeypot

Answer: D

Explanation:
Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

NEW QUESTION 112
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.



```
procs ---------memory--------swap---io--  --system-- -----cpu------
r b swpd free  buff   cache  si so bi     bo         in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040   217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003     88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20         84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0          149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0          60  431  14 1  85 0  0
```

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

A. 65
B. 77
C. 83
D. 87

Answer: D

Explanation:
The process ID 87 can be the starting point for an investigation of a possible buffer overflow attack, as it shows a high percentage of CPU utilization (99.7%) and a suspicious command name (graphic.linux_randomization.prg). A buffer overflow attack is a type of attack that exploits a vulnerability in an application or system that allows an attacker to write data beyond the allocated buffer size, potentially overwriting memory segments and executing malicious code. A high CPU utilization could indicate that the process is performing intensive or abnormal operations, such as a buffer overflow attack. A suspicious command name could indicate that the process is trying to disguise itself or evade detection, such as by mimicking a legitimate program or using random characters. The other process IDs do not show signs of a buffer overflow attack, as they have low CPU utilization and normal command names. Verified References: https://www.comptia.org/blog/what-is-buffer-overflow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 114
A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

A. Mirror the blobs at a local data center.
B. Enable fast recovery on the storage account.
C. Implement soft delete for blobs.
D. Make the blob immutable.

Answer: C

Explanation:
Soft delete allows blobs to be deleted, but the data remains accessible for a period of time before it is permanently deleted. This allows the company to delete blobs as needed, while still affording enough time for the backup process to complete. After the backup process is complete, the blobs can be permanently deleted.

NEW QUESTION 118
Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?

A. SLA
B. BIA
C. BCM
D. BCP
E. RTO

Answer: D

Explanation:
A Business Continuity Plan (BCP) is a set of policies and procedures that outline how an organization should respond to and recover from disruptions [1]. It is designed to ensure that critical operations and services can be quickly restored and maintained, and should include steps to identify risks, develop plans to mitigate those risks, and detail the procedures to be followed in the event of a disruption. Resources:
CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 4: “Business Continuity Planning,” Wiley, 2018. https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition
-p-9781119396582

NEW QUESTION 119
city government's IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:
+ Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.
+ All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.
+ Ransomware threats and zero-day vulnerabilities must be quickly identified. Which of the following technologies would BEST satisfy these requirements? (Select THREE).

A. Endpoint protection
B. Log aggregator
C. Zero trust network access
D. PAM
E. Cloud sandbox
F. SIEM
G. NGFW

Answer: BDF

Explanation:
B. Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1 .
* D. PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .
* F. SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying ransomware threats and zero- day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

NEW QUESTION 124
A company in the financial sector receives a substantial number of customer transaction requests via email. While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.

A. Implementing application blacklisting
B. Configuring the mall to quarantine incoming attachment automatically
C. Deploying host-based firewalls and shipping the logs to the SIEM
D. Increasing the cadence for antivirus DAT updates to twice daily

Answer: C

NEW QUESTION 128
A CSP, which wants to compete in the market, has been approaching companies in an attempt to gain business. The CSP is able to provide the same uptime as other CSPs at a markedly reduced cost. Which of the following would be the MOST significant business risk to a company that signs a contract with this CSP?

A. Resource exhaustion
B. Geographic location
C. Control plane breach

D. Vendor lock-in

Answer: A

Explanation:
Resource exhaustion is a condition that occurs when a system or service runs out of resources, such as memory, CPU, disk space, or bandwidth, and becomes unable to function properly or respond to requests. Resource exhaustion can be caused by high demand, poor design, misconfiguration, or malicious attacks, such as denial-of-service (DoS).
Resource exhaustion would be the most significant business risk to a company that signs a contract with a cloud service provider (CSP) that is able to provide the same uptime as other CSPs at a markedly reduced cost, because this could:
? Indicate that the CSP is oversubscribing or underprovisioning its resources, which
could result in performance degradation, service disruption, or data loss for the company.
? Affect the company's availability, reliability, and scalability requirements, which
could impact its operations, reputation, and customer satisfaction.
? Expose the company to potential security breaches or compliance violations, if the CSP does not implement adequate security controls or measures to prevent or mitigate resource exhaustion.

NEW QUESTION 131
A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of
web-application security Which of the following is the BEST option?

A. ICANN
B. PCI DSS
C. OWASP
D. CSA
E. NIST

Answer: C

NEW QUESTION 136
A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year.
Which of the following will MOST likely secure the data on the lost device?

A. Require a VPN to be active to access company data.
B. Set up different profiles based on the person's risk.
C. Remotely wipe the device.
D. Require MFA to access company applications.

Answer: C

Explanation:
Remotely wiping the device is the best way to secure the data on the lost device, as it would erase all the data and prevent unauthorized access. Requiring a VPN to be active to access company data may not protect the data on the device itself, as it could be stored locally or cached. Setting up different profiles based on the person's risk may not prevent data loss or theft, as it depends on the level of access and encryption. Requiring MFA to access company applications may not protect the data on the device itself, as it could be stored locally or cached. Verified References: https://www.comptia.org/blog/what- is-byod
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 140
A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells.
Which of the following techniques will MOST likely meet the business's needs?

A. Performing deep-packet inspection of all digital audio files
B. Adding identifying filesystem metadata to the digital audio files
C. Implementing steganography
D. Purchasing and installing a DRM suite

Answer: C

Explanation:
Steganography is a technique that can hide data within other files or media, such as images, audio, or video. This can provide a low-cost approach to theft detection for the audio recordings produced and sold by the small business, as it can embed identifying information or watermarks in the audio files that can reveal their origin or ownership. Performing deep-packet inspection of all digital audio files may not be feasible or effective for theft detection, as it could consume a lot of bandwidth and resources, and it may not detect hidden data within encrypted packets. Adding identifying filesystem metadata to the digital audio files may not provide enough protection for theft detection, as filesystem metadata can be easily modified or removed by unauthorized parties. Purchasing and installing a DRM (digital rights management) suite may not be a low-cost approach for theft detection, as it could involve licensing fees and hardware requirements. Verified References: https://www.comptia.org/blog/what-is-steganography https://partners.comptia.org/docs/default-source/resources/casp-content-guide

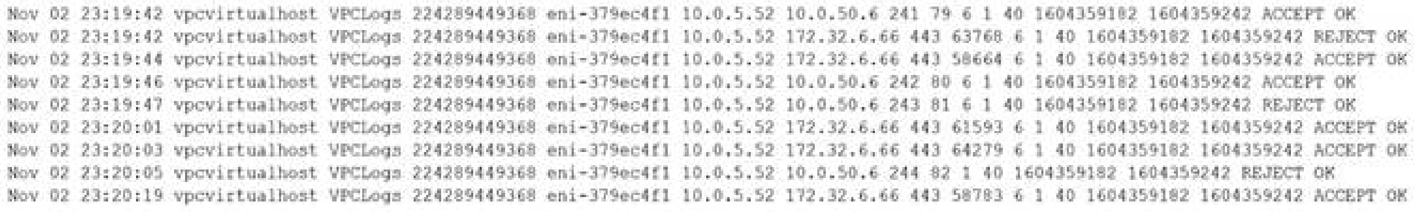
NEW QUESTION 144
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager
B. Performing DAST on a weekly basis
C. Introducing the use of container orchestration
D. Deploying instance tagging

Answer: A

Explanation:
Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/
A trusted secrets manager is a tool or service that securely stores and manages sensitive information, such as passwords, API keys, tokens, certificates, etc. A trusted secrets manager can help secure the company's CI/CD (Continuous Integration/Continuous Delivery) pipeline by preventing hard-coding sensitive environment variables in the code, which can expose them to unauthorized access or leakage. A trusted secrets manager can also enable encryption, rotation, auditing, and access control for the secrets. References: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

NEW QUESTION 146
A security analyst observes the following while looking through network traffic in a company's cloud log:



```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

A. Quarantine 10.0.5.52 and run a malware scan against the host.
B. Access 10.0.5.52 via EDR and identify processes that have network connections.
C. Isolate 10.0.50.6 via security groups.
D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Answer: D

NEW QUESTION 151
A security analyst wants to keep track of alt outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT. which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

A. X-Forwarded-Proto
B. X-Forwarded-For
C. Cache-Control
D. Strict-Transport-Security
E. Content-Security-Policy

Answer: B

NEW QUESTION 155
An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.
Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

A. Implement a VPN for all APIs.
B. Sign the key with DSA.
C. Deploy MFA for the service accounts.
D. Utilize HMAC for the keys.

Answer: D

Explanation:
Utilizing HMAC (hash-based message authentication code) for the keys is the best option for securing the REST API connection to the database while preventing the use of a hard-coded string in the request string. HMAC is a technique that uses a secret key and a hash function to generate a code that can verify the authenticity and integrity of a message, preventing unauthorized modifications or tampering. Utilizing HMAC for the keys can prevent the use of a hard-coded string in the request string, as it can dynamically generate a unique code for each request based on the secret key and the message content, making it difficult to forge or replay. Implementing a VPN (virtual private network)
for all APIs is not a good option for securing the REST API connection to the database, as it could introduce latency or performance issues for API requests, as well as not prevent the use of a hard-coded string in the request string. Signing the key with DSA (Digital Signature Algorithm) is not a good option for securing the REST API connection to the database, as it could be vulnerable to attacks or forgery if the key is compromised or weak, as well as not prevent the use of a hard-coded string in the request string. Deploying MFA (multi-factor authentication) for the service accounts is not a good option for securing the REST API connection to the database, as it could affect the usability or functionality of API requests, as well as not prevent the use of a hard-coded string in the request string. Verified References: https://www.comptia.org/blog/what-is-hmac https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 158
The OS on several servers crashed around the same time for an unknown reason. The servers were restored to working condition, and all file integrity was verified. Which of the following should the incident response team perform to understand the crash and prevent it in the future?

A. Root cause analysis
B. Continuity of operations plan
C. After-action report
D. Lessons learned

Answer: A

NEW QUESTION 161
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the

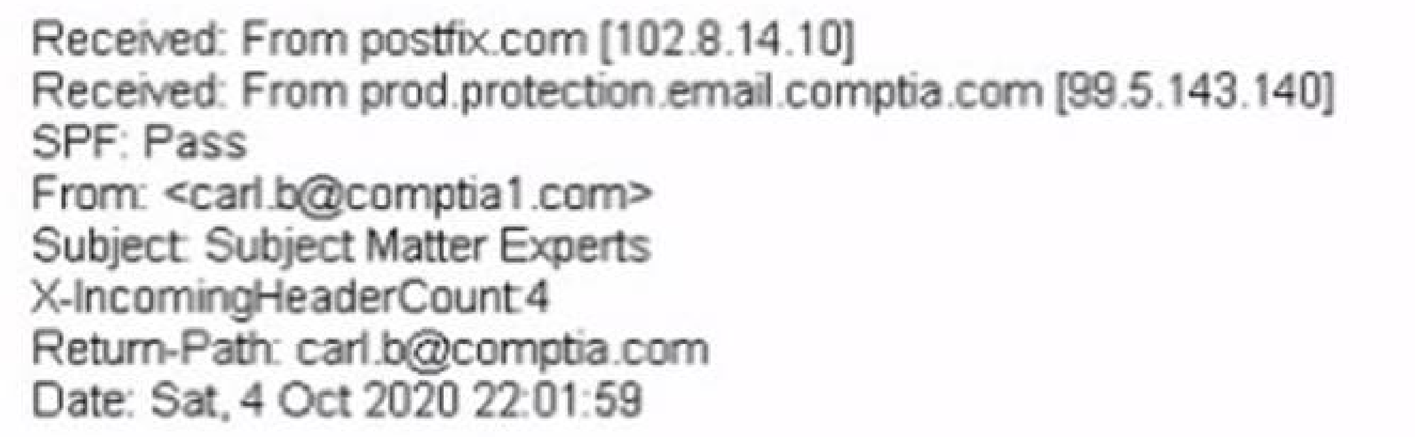
server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

Answer: A

Explanation:
Moving the server to a cloud provider is the most cost-effective solution to avoid performance issues caused by too many connections during peak seasons, such as holidays. Moving the server to a cloud provider can provide scalability, elasticity, and availability for the web server, as it can adjust its resources and capacity according to the demand and traffic. Moving the server to a cloud provider can also reduce operational and maintenance costs, as the cloud provider can handle the infrastructure and security aspects. Changing the operating system may not help avoid performance issues, as it could introduce compatibility or functionality problems, and it may not address the resource or capacity limitations. Buying a new server and creating an active-active cluster may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as complex configuration and management tasks. Upgrading the server with a new one may help avoid performance issues, but it may not be cost- effective, as it could involve hardware and software expenses, as well as migration and testing efforts. Verified References: https://www.comptia.org/blog/what-is-cloud-computing https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 162
A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:



Received: From postfix.com [102.8.14.10]
Received: From prod.protection.email.comptia.com [99.5.143.140]
SPF: Pass
From: <carl.b@comptia1.com>
Subject: Subject Matter Experts
X-IncomingHeaderCount:4
Return-Path: carl.b@comptia.com
Date: Sat, 4 Oct 2020 22:01:59

As part of the image process, which of the following is the FIRST step the analyst should take?

A. Block the email address carl b@comptia1 com, as it is sending spam to subject matter experts
B. Validate the final "Received" header against the DNS entry of the domain.
C. Compare the 'Return-Path" and "Received" fields.
D. Ignore the emails, as SPF validation is successful, and it is a false positive

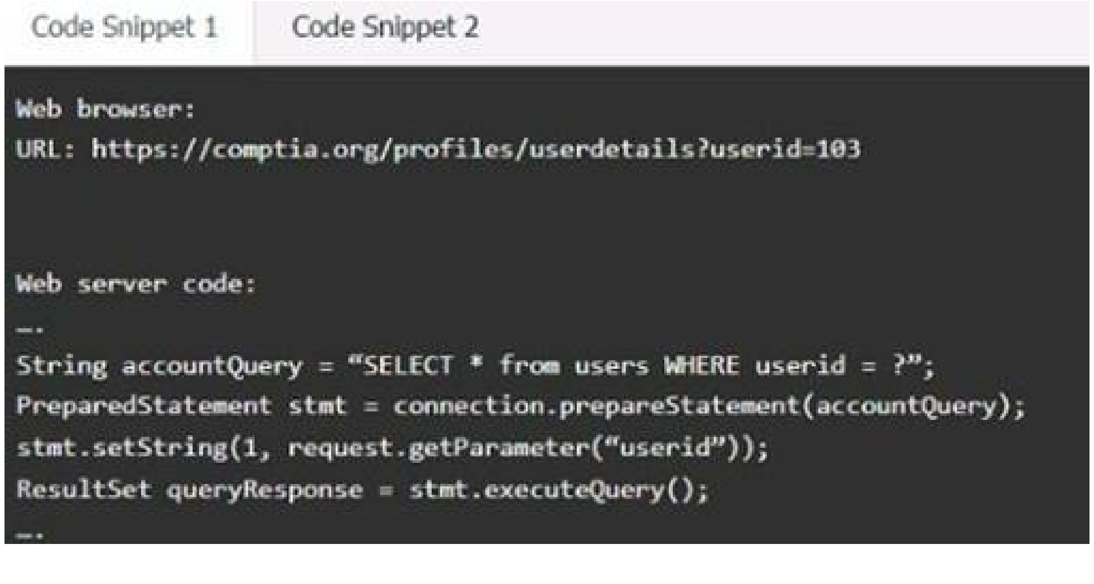
Answer: C

NEW QUESTION 165
A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company’s Linux servers. While the software version is no longer supported by the OSS community, the company’s Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.
Based on this agreement, this finding is BEST categorized as a:

A. true positive.
B. true negative.
C. false positive.
D. false negative.

Answer: C

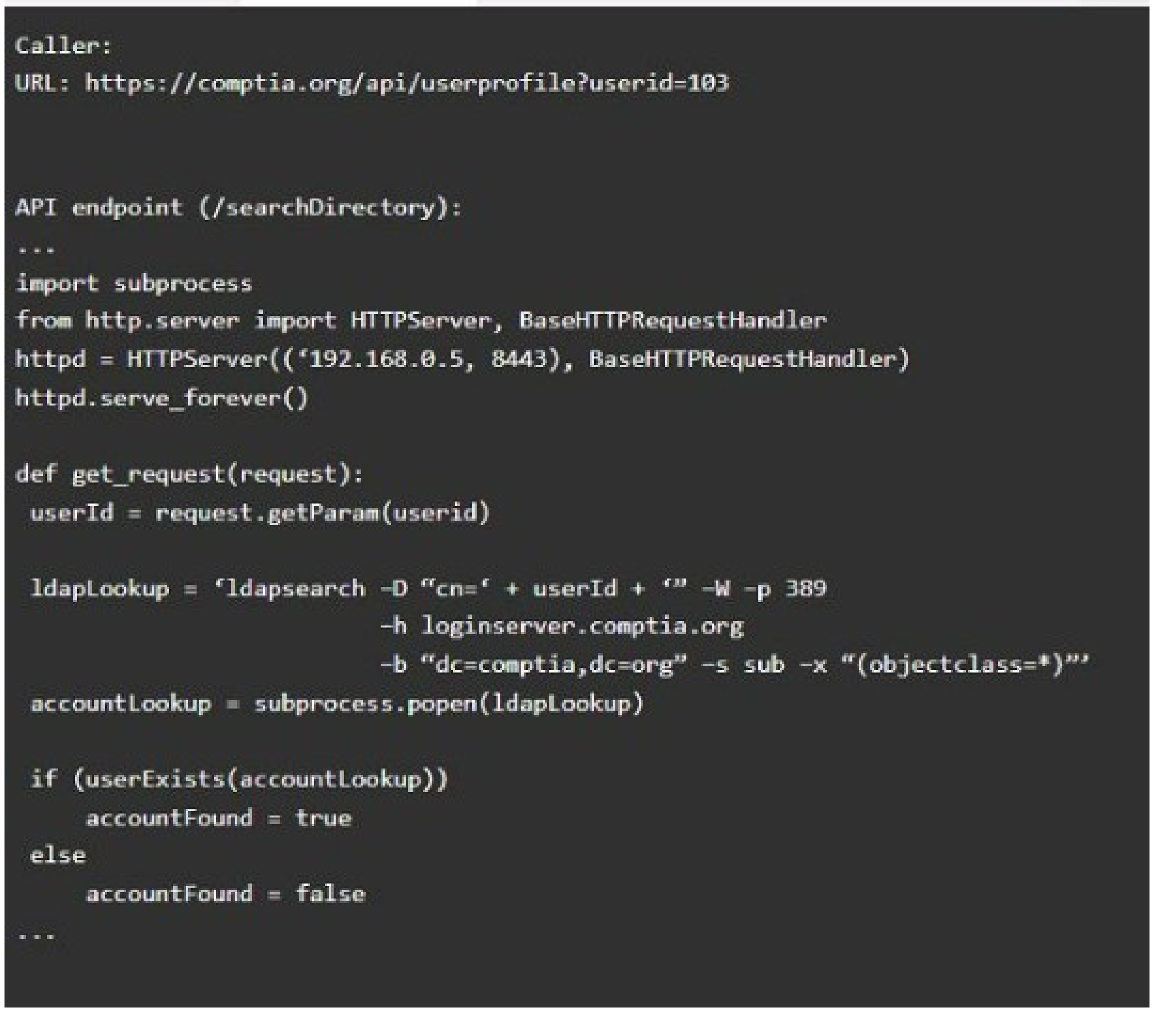
NEW QUESTION 167
SIMULATION
A product development team has submitted code snippets for review prior to release. INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1



```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
-.
String accountQuery = “SELECT * from users WHERE userid = ?”;
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter(“userid”));
ResultSet queryResponse = stmt.executeQuery();
-.
```

Code Snippet 2



```
Caller:
URL: https://comptia.org/api/userprofile?userid=103



API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                         -h loginserver.comptia.org
                         -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:
? SQL injection
? Cross-site request forgery
? Server-side request forgery
? Indirect object reference
? Cross-site scripting
Fix 1:
? Perform input sanitization of the userid field.
? Perform output encoding of queryResponse,
? Ensure usex:ia belongs to logged-in user.
? Inspect URLS and disallow arbitrary requests.
? Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind variables.
B) Remove the serve_forever instruction.
C) Prevent the "authenticated" value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

NEW QUESTION 169
Which of the following is required for an organization to meet the ISO 27018 standard?

A. All Pll must be encrypted.
B. All network traffic must be inspected.
C. GDPR equivalent standards must be met
D. COBIT equivalent standards must be met

Answer: A

NEW QUESTION 170
A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:
Work at the application layer
Send alerts on attacks from both privileged and malicious users Have a very low false positive
Which of the following should the architect recommend?

A. FIM
B. WAF
C. NIPS
D. DAM
E. UTM

Answer: D

NEW QUESTION 174
Company A acquired Company B. During an initial assessment, the companies discover they are using the same SSO system. To help users with the transition, Company A is requiring the following:
• Before the merger is complete, users from both companies should use a single set of usernames and passwords.
• Users in the same departments should have the same set of rights and privileges, but they should have different sets of rights and privileges if they have different IPs.
• Users from Company B should be able to access Company A's available resources. Which of the following are the BEST solutions? (Select TWO).

A. Installing new Group Policy Object policies
B. Establishing one-way trust from Company B to Company A
C. Enabling multifactor authentication
D. Implementing attribute-based access control
E. Installing Company A's Kerberos systems in Company B's network
F. Updating login scripts

Answer: BD

Explanation:
Establishing one-way trust from Company B to Company A would allow users from Company B to access Company A's resources using their existing credentials. Implementing attribute-based access control would allow users to have different sets of rights and privileges based on their attributes, such as department and IP address. Verified References:
- https://www.cloudflare.com/learning/access-management/what-is-sso/
- https://frontegg.com/blog/a-complete-guide-to-implementing-single-sign-on
- https://learn.microsoft.com/en-us/host-integration-server/esso/enterprise-single-sign-on-basics

NEW QUESTION 176
A network administrator for a completely air-gapped and closed system has noticed that anomalous external files have been uploaded to one of the critical servers. The administrator has reviewed logs in the SIEM that were collected from security appliances, network infrastructure devices, and endpoints. Which of the following processes, if executed, would be MOST likely to expose an attacker?

A. Reviewing video from IP cameras within the facility
B. Reconfiguring the SIEM connectors to collect data from the perimeter network hosts
C. Implementing integrity checks on endpoint computing devices
D. Looking for privileged credential reuse on the network

Answer: A

Explanation:
Reviewing video from IP cameras within the facility would be the most likely process to expose an attacker who has compromised an air-gapped system. Since air-gapped systems are isolated from external networks, an attacker would need physical access to the system or use some covert channel to communicate with it. Video surveillance could reveal any unauthorized or suspicious activity within the facility that could be related to the attack. Verified References:
- https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
- https://en.wikipedia.org/wiki/Air-Gap_Malware
- https://www.techtarget.com/searchsecurity/essentialguide/How-air-gap-attacks-challenge-the-notion-of-se

NEW QUESTION 180
A company wants to implement a new website that will be accessible via browsers with no mobile applications available. The new website will allow customers to submit sensitive medical information securely and receive online medical advice. The company already has multiple other websites where it provides various public health data and information. The new website must implement the following:
• The highest form Of web identity validation
• Encryption of all web transactions
• The strongest encryption in-transit
• Logical separation based on data sensitivity Other things that should be considered include:
• The company operates multiple other websites that use encryption.
• The company wants to minimize total expenditure.

• The company wants to minimize complexity
Which of the following should the company implement on its new website? (Select TWO).

A. Wildcard certificate
B. EV certificate
C. Mutual authentication
D. Certificate pinning
E. SSO
F. HSTS

Answer: BF

Explanation:
The company should implement an EV certificate and HSTS on its new website. An EV certificate provides the highest level of web identity validation by requiring extensive verification of the organization's identity and domain ownership. HSTS enforces encryption of all web transactions by redirecting HTTP requests to HTTPS and preventing users from accepting invalid certificates. These solutions would enhance the security and trustworthiness of the website without increasing complexity or expenditure significantly. Verified References:

- https://www.entrust.com/digital-security/certificate-solutions/products/digital-certificates/tls-ssl-certificate
- https://learn.microsoft.com/en-us/azure/active-directory/develop/access-tokens

NEW QUESTION 181
A network administrator receives a ticket regarding an error from a remote worker who is trying to reboot a laptop. The laptop has not yet loaded the operating system, and the user is unable to continue the boot process. The administrator is able to provide the user with a recovery PIN, and the user is able to reboot the system and access the device as needed. Which of the following is the MOST likely cause of the error?

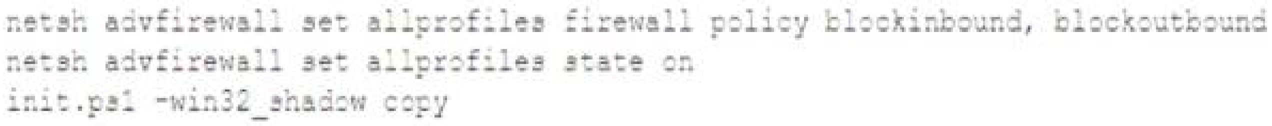
A. Lockout of privileged access account
B. Duration of the BitLocker lockout period
C. Failure of the Kerberos time drift sync
D. Failure of TPM authentication

Answer: D

Explanation:
The most likely cause of the error is the failure of TPM authentication. TPM stands for Trusted Platform Module, which is a hardware component that stores encryption keys and other security information. TPM can be used by BitLocker to protect the encryption keys and verify the integrity of the boot process. If TPM fails to authenticate the laptop, BitLocker will enter recovery mode and ask for a recovery PIN, which is a 48-digit numerical password that can be used to unlock the system. The administrator should check the TPM status and configuration and make sure it is working properly. Verified References:

- https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27-
- https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bi
- https://docs.sophos.com/esg/sgn/8-1/user/win/en-us/esg/SafeGuard-Enterprise/tasks/BitLockerRecoveryK

NEW QUESTION 186
A security researcher detonated some malware in a lab environment and identified the following commands running from the EDR tool:



```
netsh advfirewall set allprofiles firewall policy blockinbound, blockoutbound
netsh advfirewall set allprofiles state on
init.ps1 -win32_shadow copy
```

With which of the following MITRE ATT&CK TTPs is the command associated? (Select TWO).

A. Indirect command execution
B. OS credential dumping
C. Inhibit system recovery
D. External remote services
E. System information discovery
F. Network denial of service

Answer: BE

Explanation:
OS credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. System information discovery is the process of gathering information about the system, such as hostname, IP address, OS version, running processes, etc. Both of these techniques are commonly used by adversaries to gain access to sensitive data and resources on the target system. The command shown in the image is using Mimikatz, a tool that can dump credentials from memory, and also querying the system information using WMIC. Verified References:

- https://attack.mitre.org/techniques/T1003/
- https://attack.mitre.org/techniques/T1082/
- https://github.com/gentilkiwi/mimikatz
- https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmic

NEW QUESTION 191
A local university that has a global footprint is undertaking a complete overhaul of its website and associated systems. Some of the requirements are:
• Handle an increase in customer demand of resources
• Provide quick and easy access to information
• Provide high-quality streaming media
• Create a user-friendly interface
Which of the following actions should be taken FIRST?

A. Deploy high-availability web server
B. Enhance network access controls.
C. Implement a content delivery networ
D. Migrate to a virtualized environment.

Answer: C

Explanation:
A content delivery network (CDN) is a geographically distributed network of servers that can cache content close to end users, allowing for faster and more efficient delivery of web content, such as images, videos, and streaming media. A CDN can also handle an increase in customer demand of resources, provide high-quality streaming media, and create a user-friendly interface by reducing latency and bandwidth consumption. A CDN can also improve the security and availability of the website by mitigating DDoS attacks and providing redundancy. Verified References:

- https://www.cloudflare.com/learning/cdn/what-is-a-cdn/
- https://learn.microsoft.com/en-us/azure/cdn/cdn-overview
- https://en.wikipedia.org/wiki/Content_delivery_network

NEW QUESTION 194
An organization is looking to establish more robust security measures by implementing PKI. Which of the following should the security analyst implement when considering mutual authentication?

A. Perfect forward secrecy on both endpoints
B. Shared secret for both endpoints
C. Public keys on both endpoints
D. A common public key on each endpoint
E. A common private key on each endpoint

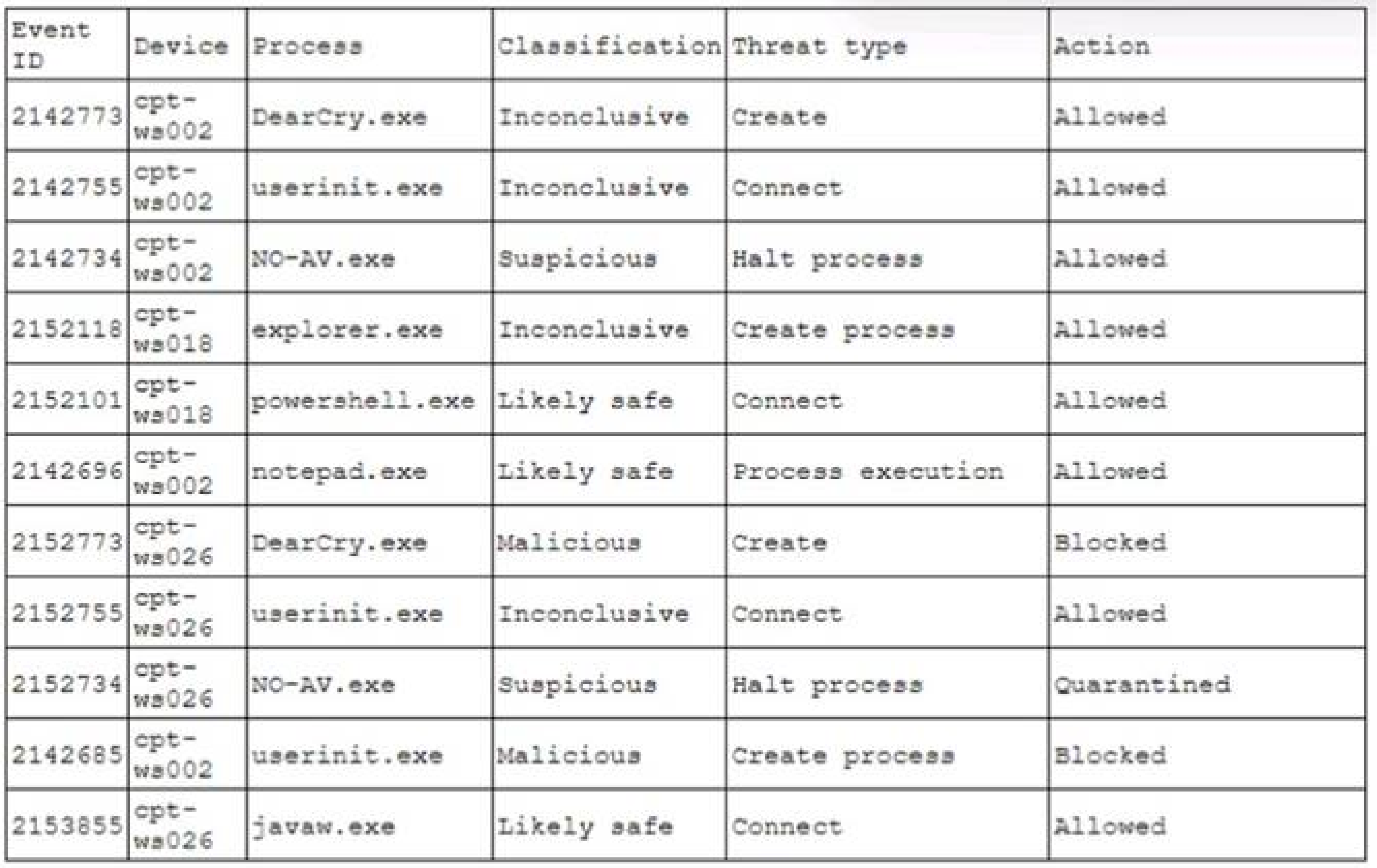
Answer: C

Explanation:
Public keys on both endpoints are required for implementing PKI-based mutual authentication. PKI stands for Public Key Infrastructure, which is a system that manages the creation, distribution, and verification of certificates. Certificates are digital documents that contain public keys and identity information of their owners. Certificates are issued by trusted authorities called Certificate Authorities (CAs), and can be used to prove the identity and authenticity of the certificate holders. Mutual authentication is a process in which two parties authenticate each other at the same time using certificates. Mutual authentication can provide stronger security and privacy than one-way authentication, where only one party is authenticated. In PKI-based mutual authentication, each party has a certificate that contains its public key and identity information, and a private key that corresponds to its public key. The private key is kept secret and never shared with anyone, while the public key is shared and used to verify the identity and signature of the certificate holder. The basic steps of PKI-based mutual authentication are as follows:

- Party A sends its certificate to Party B.
- Party B verifies Party A’s certificate by checking its validity, signature, and trust chain. If the certificate is valid and trusted, Party B extracts Party A’s public key from the certificate.
- Party B generates a random challenge (such as a nonce or a timestamp) and encrypts it with Party A’s public key. Party B sends the encrypted challenge to Party A.
- Party A decrypts the challenge with its private key and sends it back to Party B.
- Party B compares the received challenge with the original one. If they match, Party B confirms that Party A is the legitimate owner of the certificate and has possession of the private key.
- The same steps are repeated in reverse, with Party A verifying Party B’s certificate and sending a challenge encrypted with Party B’s public key.

* A. Perfect forward secrecy on both endpoints is not required for implementing PKI-based mutual authentication. Perfect forward secrecy (PFS) is a property of encryption protocols that ensures that the compromise of a long-term secret key (such as a private key) does not affect the security of past or future session keys (such as symmetric keys). PFS can enhance the security and privacy of encrypted communications, but it does not provide authentication by itself.
* B. Shared secret for both endpoints is not required for implementing PKI-based mutual authentication. Shared secret is a method of authentication that relies on a pre-shared piece of information (such as a password or a passphrase) that is known only to both parties. Shared secret can provide simple and fast authentication, but it does not provide non-repudiation or identity verification.
* D. A common public key on each endpoint is not required for implementing PKI-based mutual authentication. A common public key on each endpoint would imply that both parties share the same certificate and private key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.
* E. A common private key on each endpoint is not required for implementing PKI-based mutual authentication. A common private key on each endpoint would imply that both parties share the same certificate and public key, which would defeat the purpose of PKI-based mutual authentication. Each party should have its own unique certificate and private key that proves its identity and authenticity.

NEW QUESTION 199
A pharmaceutical company was recently compromised by ransomware. Given the following EDR output from the process investigation:



Event ID	Device	Process	Classification	Threat type	Action
2142773	cpt-ws002	DearCry.exe	Inconclusive	Create	Allowed
2142755	cpt-ws002	userinit.exe	Inconclusive	Connect	Allowed
2142734	cpt-ws002	NO-AV.exe	Suspicious	Halt process	Allowed
2152118	cpt-ws018	explorer.exe	Inconclusive	Create process	Allowed
2152101	cpt-ws018	powershell.exe	Likely safe	Connect	Allowed
2142696	cpt-ws002	notepad.exe	Likely safe	Process execution	Allowed
2152773	cpt-ws026	DearCry.exe	Malicious	Create	Blocked
2152755	cpt-ws026	userinit.exe	Inconclusive	Connect	Allowed
2152734	cpt-ws026	NO-AV.exe	Suspicious	Halt process	Quarantined
2142685	cpt-ws002	userinit.exe	Malicious	Create process	Blocked
2153855	cpt-ws026	javaw.exe	Likely safe	Connect	Allowed

On which of the following devices and processes did the ransomware originate?

A. cpt-ws018, powershell.exe
B. cpt-ws026, DearCry.exe
C. cpt-ws002, NO-AV.exe
D. cpt-ws026, NO-AV.exe
E. cpt-ws002, DearCry.exe

Answer: D

Explanation:

The EDR output shows the process tree of the ransomware infection. The root node is NO- AV.exe, which is a malicious executable that disables antivirus software and downloads the DearCry ransomware. The NO-AV.exe process was launched on cpt-ws026 by a user named John. The DearCry.exe process was then launched on cpt-ws026 by NO-AV.exe and propagated to other devices via SMB. Therefore, the ransomware originated from cpt- ws026 and NO-AV.exe.
Verified References:
? https://www.microsoft.com/security/blog/2021/03/12/analyzing-dearcry-ransomware-the-first-attack-to-exploit-exchange-server-vulnerabilities/
? https://www.crowdstrike.com/blog/dearcry-ransomware-analysis/

NEW QUESTION 204
A security architect is tasked with securing a new cloud-based videoconferencing and collaboration platform to support a new distributed workforce. The security architect's key objectives are to:
• Maintain customer trust
• Minimize data leakage
• Ensure non-repudiation
Which of the following would be the BEST set of recommendations from the security architect?

A. Enable the user authentication requirement, enable end-to-end encryption, and enable waiting rooms.
B. Disable file exchange, enable watermarking, and enable the user authenticationrequirement.
C. Enable end-to-end encryption, disable video recording, and disable file exchange.
D. Enable watermarking, enable the user authentication requirement, and disable video recording.

Answer: B

Explanation:

Disabling file exchange can help to minimize data leakage by preventing users from sharing sensitive documents or data through the videoconferencing platform. Enabling watermarking can help to maintain customer trust and ensure non-repudiation by adding a visible or invisible mark to the video stream that identifies the source or owner of the content. Enabling the user authentication requirement can help to secure the videoconferencing sessions by verifying the identity of the participants and preventing unauthorized access. Verified References:
? https://www.rev.com/blog/marketing/follow-these-7-video-conferencing-security-best-practices
? https://www.paloaltonetworks.com/blog/2020/04/network-video-conferencing- security/
? https://www.megameeting.com/news/best-practices-secure-video-conferencing/

NEW QUESTION 205
The Chief Information Security Officer (CISO) asked a security manager to set up a system that sends an alert whenever a mobile device enters a sensitive area of the company's data center. The CISO would also like to be able to alert the individual who is entering the area that the access was logged and monitored. Which of the following would meet these requirements?

A. Near-field communication
B. Short Message Service
C. Geofencing
D. Bluetooth

Answer: C

Explanation:

Geofencing is a location-based service that allows an organization to define and enforce a virtual boundary around a sensitive area, such as a data center. Geofencing can use various technologies, such as GPS, Wi-Fi, cellular data, or RFID, to detect when a mobile device enters or exits the geofence. Geofencing can also trigger certain actions or notifications based on the device's location. For example, the organization can set up a geofencing policy that sends an alert to the CISO and the device user when a mobile device enters the data center area. Geofencing can also be used to restrict access to certain apps or features based on the device's location. Verified References:
? https://developer.android.com/training/location/geofencing
? https://www.manageengine.com/mobile-device-management/mdm- geofencing.html
? https://www.koombea.com/blog/mobile-geofencing/

NEW QUESTION 209
A security analyst for a managed service provider wants to implement the most up-to-date and effective security methodologies to provide clients with the best offerings. Which of the following resources would the analyst MOST likely adopt?

A. OSINT
B. ISO
C. MITRE ATT&CK
D. OWASP

Answer: C

Explanation:

MITRE ATT&CK is a threat management framework that provides a comprehensive and detailed knowledge base of adversary tactics and techniques based on real-world observations. It can help security analysts to identify, understand, and prioritize potential threats, as well as to develop effective detection and response strategies. MITRE ATT&CK covers the entire lifecycle of a cyberattack, from initial access to impact, and provides information on how to mitigate, detect, and hunt for each technique. It also includes threat actor profiles, software descriptions, and data sources that can be used for threat intelligence and analysis. MITRE ATT&CK is the most likely resource that a security analyst would adopt to implement the most up-to-date and effective security methodologies for their clients.
Verified References:
? https://attack.mitre.org/
? https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/

NEW QUESTION 212
Which of the following is a risk associated with SDN?

A. Expanded attack surface
B. Increased hardware management costs
C. Reduced visibility of scaling capabilities
D. New firmware vulnerabilities

Answer: A

Explanation:

A risk associated with SDN is the expanded attack surface that it introduces. SDN is a network architecture that decouples the control plane from the data plane, allowing centralized and programmable management of network devices and traffic. However, this also exposes new attack vectors and vulnerabilities that can compromise the security and performance of the network. For example, an attacker can target the SDN controller, which is the core component that communicates with and controls the network devices. A successful attack on the SDN controller can result in denial of service, unauthorized access, data leakage, or network hijacking. An attacker can also exploit the communication channels between the SDN controller and the network devices, such as the OpenFlow protocol, to intercept, modify, or inject malicious messages or commands. Additionally, an attacker can leverage malicious or compromised applications that run on top of the SDN controller to manipulate or disrupt the network behavior. Verified References:
? https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/benefits-and-the-security-risk-of-software-defined-networking
? https://link.springer.com/article/10.1007/s40860-022-00171-8

NEW QUESTION 213
......