CAS-003.142q

Number: CAS-003
Passing Score: 800
Time Limit: 120 min

CAS-003

CompTIA Advanced Security Practitioner (CASP)

Exam A

QUESTION 1
Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication
Network Server: Digitally sign communication

A storage administrator in a remote location with a legacy storage array, which contains time-sensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgraded
B. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgraded
C. Mitigate the risk for the remote location by suggesting a move to a cloud service provider. Have the remote location request an indefinite risk exception for the use of cloud storage
D. Avoid the risk, leave the settings alone, and decommission the legacy storage device

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

A. Set up a VDI environment that prevents copying and pasting to the local workstations of outsourced staff members
B. Install a client-side VPN on the staff laptops and limit access to the development network
C. Create an IPSec VPN tunnel from the development network to the office of the outsourced staff

D. Use online collaboration tools to initiate workstation-sharing sessions with local staff who have access to the development network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

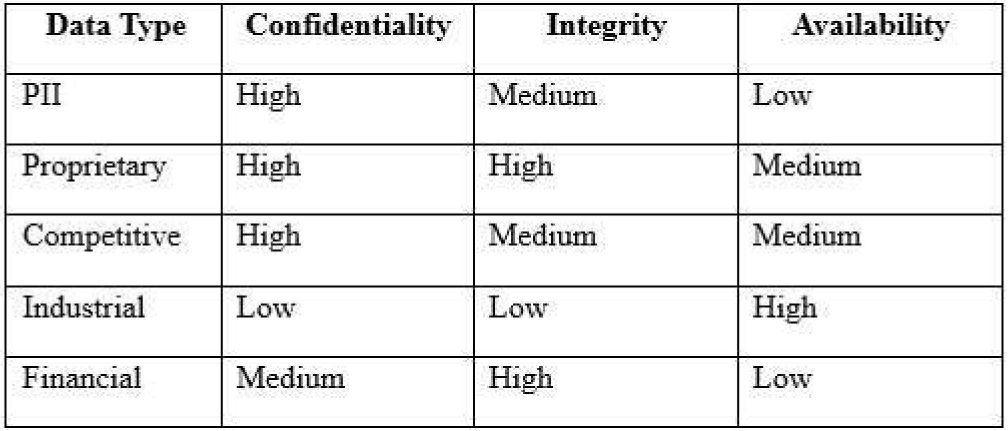
QUESTION 3
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploited so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions.
Which of the following approaches is described?

A. Blue team
B. Red team
C. Black box
D. White team

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://resources.infosecinstitute.com/the-types-of-penetration-testing/#gref

QUESTION 4
An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.



Data Type	Confidentiality	Integrity	Availability
PII	High	Medium	Low
Proprietary	High	High	Medium
Competitive	High	Medium	Medium
Industrial	Low	Low	High
Financial	Medium	High	Low

Based on the data classification table above, which of the following BEST describes the overall classification?

A. High confidentiality, high availability
B. High confidentiality, medium availability
C. Low availability, low confidentiality
D. High integrity, low availability

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization’s users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

A. OTA updates
B. Remote wiping
C. Side loading

D. Sandboxing
E. Containerization
F. Signed applications

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A security incident responder discovers an attacker has gained access to a network and has overwritten key system files with backdoor software. The server was reimaged and patched offline. Which of the following tools should be implemented to detect similar attacks?

A. Vulnerability scanner
B. TPM
C. Host-based firewall
D. File integrity monitor
E. NIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents.
The following observations have been identified:

1. The ICS supplier has specified that any software installed will result in lack of support.
2. There is no documented trust boundary defined between the SCADA and corporate networks.
3. Operational technology staff have to manage the SCADA equipment via the engineering workstation.
4. There is a lack of understanding of what is within the SCADA network.

Which of the following capabilities would BEST improve the security position?

A. VNC, router, and HIPS

B. SIEM, VPN, and firewall
C. Proxy, VPN, and WAF
D. IDS, NAC, and log monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

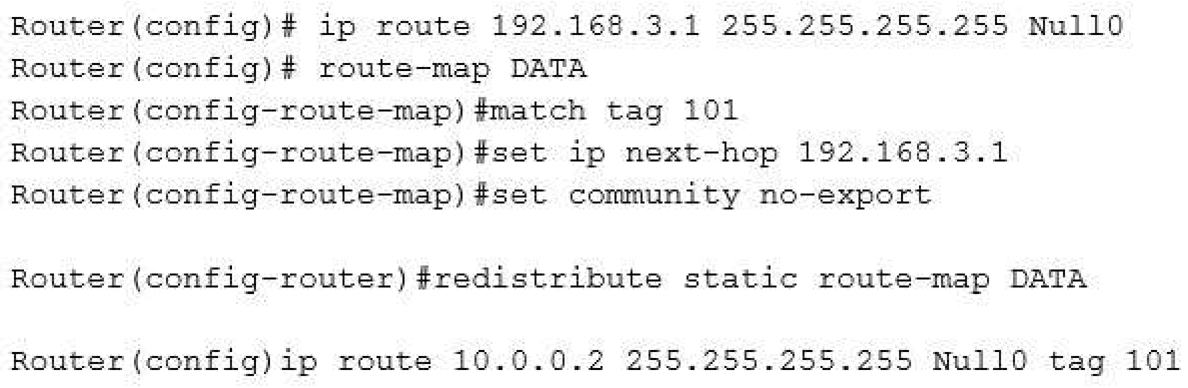
QUESTION 8
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:



```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
Router(config)# route-map DATA
Router(config-route-map)#match tag 101
Router(config-route-map)#set ip next-hop 192.168.3.1
Router(config-route-map)#set community no-export

Router(config-router)#redistribute static route-map DATA

Router(config)ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

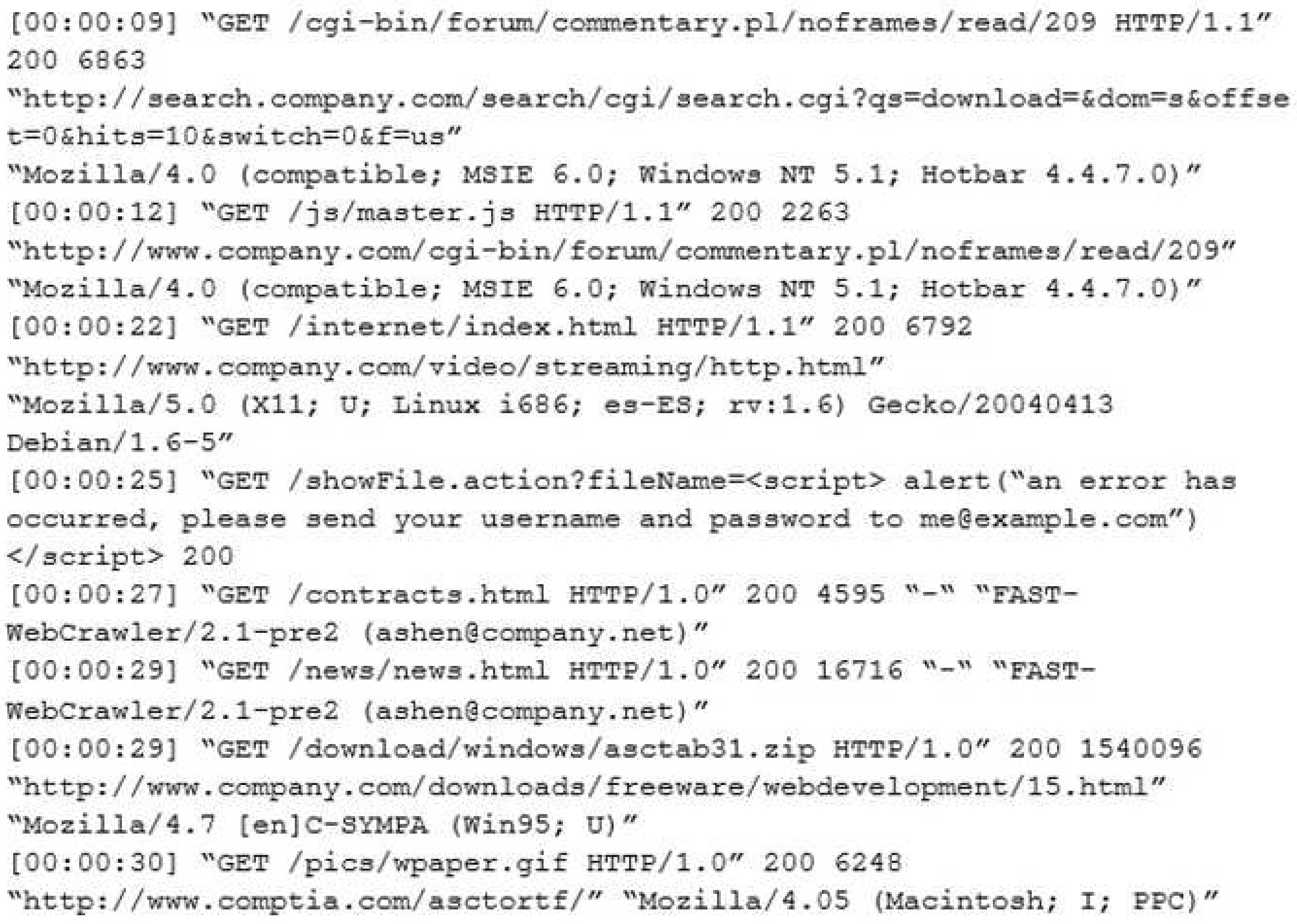
Which of the following is the engineer implementing?

A. Remotely triggered black hole
B. Route protection
C. Port security
D. Transport security
E. Address space layout randomization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.



```
[00:00:09] “GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1”
200 6863
“http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offse
t=0&hits=10&switch=0&f=us”
“Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)”
[00:00:12] “GET /js/master.js HTTP/1.1” 200 2263
“http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209”
“Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)”
[00:00:22] “GET /internet/index.html HTTP/1.1” 200 6792
“http://www.company.com/video/streaming/http.html”
“Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5”
[00:00:25] “GET /showFile.action?fileName=<script> alert(“an error has
occurred, please send your username and password to me@example.com”)
</script> 200
[00:00:27] “GET /contracts.html HTTP/1.0” 200 4595 “-“ “FAST-
WebCrawler/2.1-pre2 (ashen@company.net)”
[00:00:29] “GET /news/news.html HTTP/1.0” 200 16716 “-“ “FAST-
WebCrawler/2.1-pre2 (ashen@company.net)”
[00:00:29] “GET /download/windows/asctab31.zip HTTP/1.0” 200 1540096
“http://www.company.com/downloads/freeware/webdevelopment/15.html”
“Mozilla/4.7 [en]C-SYMPA (Win95; U)”
[00:00:30] “GET /pics/wpaper.gif HTTP/1.0” 200 6248
“http://www.comptia.com/asctortf/” “Mozilla/4.05 (Macintosh; I; PPC)”
```

Which of the following types of attack vector did the penetration tester use?

A. SQL injection
B. CSRF
C. Brute force
D. XSS
E. TOC/TOU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristics for anomaly detection
D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

A. Vulnerability assessment
B. Risk assessment
C. Patch management
D. Device quarantine
E. Incident management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A systems administrator at a medical imaging company discovers protected health information (PHI) on a general-purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2
B. Immediately encrypt all PHI with AES 256
C. Delete all PHI from the network until the legal department is consulted
D. Consult the legal department to determine legal requirements

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:

- High-impact controls implemented: 6 out of 10
- Medium-impact controls implemented: 409 out of 472
- Low-impact controls implemented: 97 out of 1000

The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:

- Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000
- Average medium-impact control implementation cost: $6,250; Probable ALE for each medium-impact control gap: $11,000

Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the past
B. The enterprise security team has focused exclusively on mitigating high-level risks
C. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controls
D. The cybersecurity team has balanced residual risk for both high and medium controls

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit. Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence. The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?

A. Update and deploy GPOs
B. Configure and use measured boot
C. Strengthen the password complexity requirements
D. Update the antivirus software and definitions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client-facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

A. Install a HIPS on the web servers
B. Disable inbound traffic from offending sources
C. Disable SNMP on the web servers
D. Install anti-DDoS protection in the DMZ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
One of the objectives of a bank is to instill a security awareness culture. Which of the following are techniques that could help to achieve this? (Choose two.)

A. Blue teaming
B. Phishing simulations
C. Lunch-and-learn
D. Random audits
E. Continuous monitoring
F. Separation of duties

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
D. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

A. Magic link sent to an email address
B. Customer ID sent via push notification

C. SMS with OTP sent to a mobile number
D. Third-party social login
E. Certificate sent to be installed on a device
F. Hardware tokens sent to customers

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

- The tool needs to be responsive so service teams can query it, and then perform an automated response action.
- The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
- The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

A. Review the CVE database for critical exploits over the past year
B. Use social media to contact industry analysts
C. Use intelligence gathered from the Internet relay chat channels
D. Request information from security vendors and government agencies
E. Perform a penetration test of the competitor’s network and share the results with the board

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO’s request?

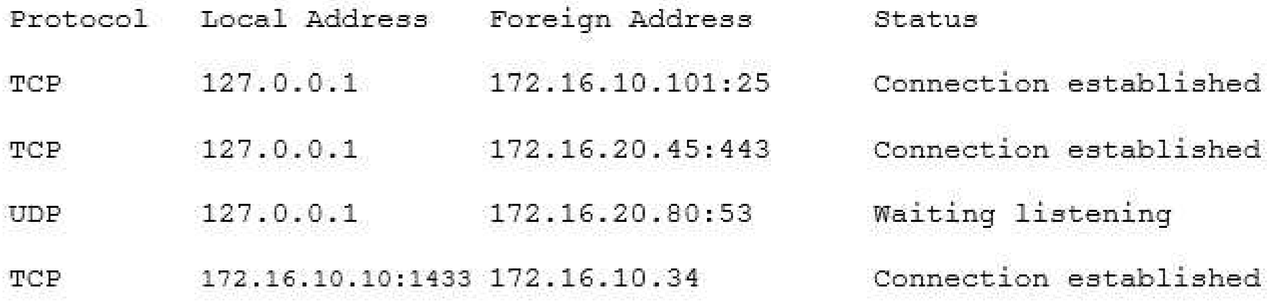
A. 1. Perform the ongoing research of the best practices
2. Determine current vulnerabilities and threats
3. Apply Big Data techniques
4. Use antivirus control
B. 1. Apply artificial intelligence algorithms for detection
2. Inform the CERT team
3. Research threat intelligence and potential adversaries
4. Utilize threat intelligence to apply Big Data techniques
C. 1. Obtain the latest IOCs from the open source repositories
2. Perform a sweep across the network to identify positive matches
3. Sandbox any suspicious files
4. Notify the CERT team to apply a future proof threat model

D. 1. Analyze the current threat intelligence
   2. Utilize information sharing to obtain the latest industry IOCs
   3. Perform a sweep across the network to identify positive matches
   4. Apply machine learning algorithms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information:



```
Protocol    Local Address      Foreign Address       Status

TCP         127.0.0.1          172.16.10.101:25      Connection established

TCP         127.0.0.1          172.16.20.45:443      Connection established

UDP         127.0.0.1          172.16.20.80:53       Waiting listening

TCP         172.16.10.10:1433  172.16.10.34          Connection established
```

Which of the following commands would have provided this output?

A. `arp -s`
B. `netstat -a`
C. `ifconfig -arp`
D. `sqlmap -w`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Management is reviewing the results of a recent risk assessment of the organization’s policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

A. Transfer
B. Mitigate
C. Accept
D. Avoid
E. Reject

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:

```
^32^[34fda19(fd^43gfd/home/user/lib/module.so.343jk^rfw(342fds43g
```

Which of the following did the analyst use to determine the location of the malicious payload?

A. Code deduplicators
B. Binary reverse-engineering
C. Fuzz testing
D. Security containers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

A. Inform the customer that the service provider does not have any control over third-party blacklist entries. The customer should reach out to the blacklist operator directly
B. Perform a takedown of any customer accounts that have entries on email blacklists because this is a strong indicator of hostile behavior
C. Work with the legal department and threaten legal action against the blacklist operator if the netblocks are not removed because this is affecting legitimate traffic
D. Establish relationship with a blacklist operators so broad entries can be replaced with more granular entries and incorrect entries can be quickly pruned

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
An agency has implemented a data retention policy that requires tagging data according to type before storing it in the data repository. The policy requires all business emails be automatically deleted after two years. During an open records investigation, information was found on an employee’s work computer concerning a conversation that occurred three years prior and proved damaging to the agency’s reputation. Which of the following MOST likely caused the data leak?

A. The employee manually changed the email client retention settings to prevent deletion of emails
B. The file that contained the damaging information was mistagged and retained on the server for longer than it should have been
C. The email was encrypted and an exception was put in place via the data classification application
D. The employee saved a file on the computer’s hard drive that contained archives of emails, which were more than two years old

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
A forensics analyst suspects that a breach has occurred. Security logs show the company’s OS patch system may be compromised, and it is serving patches that contain a zero-day exploit and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server. Which of the following should the analyst use to confirm this suspicion?

A. File size
B. Digital signature
C. Checksums
D. Anti-malware software
E. Sandboxing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A company is acquiring incident response and forensic assistance from a managed security service provider in the event of a data breach. The company has selected a partner and must now provide required documents to be reviewed and evaluated. Which of the following documents would BEST protect the company and ensure timely assistance? (Choose two.)

A. RA
B. BIA
C. NDA
D. RFI
E. RFQ
F. MSA

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

A. Issue digital certificates to all users, including owners of group mailboxes, and enable S/MIME

B. Federate with an existing PKI provider, and reject all non-signed emails
C. Implement two-factor email authentication, and require users to hash all email messages upon receipt
D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems
B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack. Which of the following business documents would be BEST to document this engagement?

A. Business partnership agreement
B. Memorandum of understanding
C. Service-level agreement
D. Interconnection security agreement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-47.pdf

QUESTION 33
A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development. Which of the following SDLC best practices should the development team have followed?

A. Implementing regression testing
B. Completing user acceptance testing
C. Verifying system design documentation
D. Using a SRTM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

A. Exempt mobile devices from the requirement, as this will lead to privacy violations
B. Configure the devices to use an always-on IPSec VPN
C. Configure all management traffic to be tunneled into the enterprise via TLS
D. Implement a VDI solution and deploy supporting client apps to devices
E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35

After multiple service interruptions caused by an older datacenter design, a company decided to migrate away from its datacenter. The company has successfully completed the migration of all datacenter servers and services to a cloud provider. The migration project includes the following phases:

- Selection of a cloud provider
- Architectural design
- Microservice segmentation
- Virtual private cloud
- Geographic service redundancy
- Service migration

The Chief Information Security Officer (CISO) is still concerned with the availability requirements of critical company applications. Which of the following should the company implement NEXT?

A. Multicloud solution

B. Single-tenancy private cloud

C. Hybrid cloud solution

D. Cloud access security broker

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36

A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: `“<object object_ref=… />”` and `“<state state_ref=… />”.` Which of the following tools BEST supports the use of these definitions?

A. HTTP interceptor

B. Static code analyzer

C. SCAP scanner

D. XML fuzzer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization:

```
localStorage.setItem(“session-cookie”, document.cookie);
```

Which of the following should the security engineer recommend?

A. SessionStorage should be used so authorized cookies expire after the session ends
B. Cookies should be marked as “secure” and “HttpOnly”
C. Cookies should be scoped to a relevant domain/path
D. Client-side cookies should be replaced by server-side mechanisms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A hospital’s security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer (CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been

remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

A. When it is mandated by their legal and regulatory requirements
B. As soon as possible in the interest of the patients
C. As soon as the public relations department is ready to be interviewed
D. When all steps related to the incident response plan are completed
E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
A deployment manager is working with a software development group to assess the security of a new version of the organization's internally developed ERP tool. The organization prefers to not perform assessment activities following deployment, instead focusing on assessing security throughout the life cycle. Which of the following methods would BEST assess the security of the product?

A. Static code analysis in the IDE environment
B. Penetration testing of the UAT environment
C. Vulnerability scanning of the production environment
D. Penetration testing of the production environment
E. Peer review prior to unit testing

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
During a security event investigation, a junior analyst fails to create an image of a server's hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

A. Continuity of operations
B. Chain of custody
C. Order of volatility
D. Data recovery

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.computer-forensics-recruiter.com/order-of-volatility/

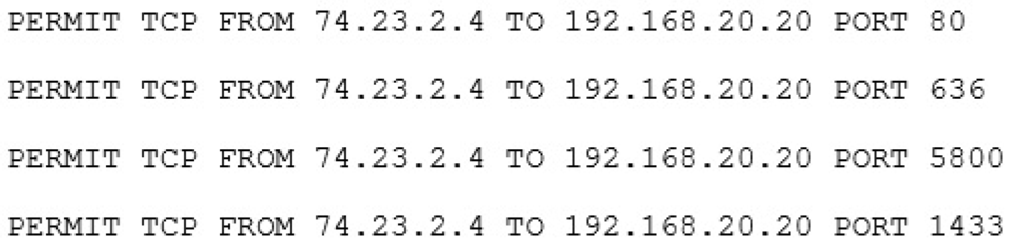
QUESTION 42
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (CIO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

A. Multi-tenancy SaaS
B. Hybrid IaaS
C. Single-tenancy PaaS
D. Community IaaS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a third-party service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:



```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?

A. LDAP
B. WAYF
C. OpenID
D. RADIUS
E. SAML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources. Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

A. Isolate the systems on their own network
B. Install a firewall and IDS between systems and the LAN
C. Employ own stratum-0 and stratum-1 NTP servers
D. Upgrade the software on critical systems
E. Configure the systems to use government-hosted NTP servers

Correct Answer: BE
Section: (none)

Explanation

Explanation/Reference:

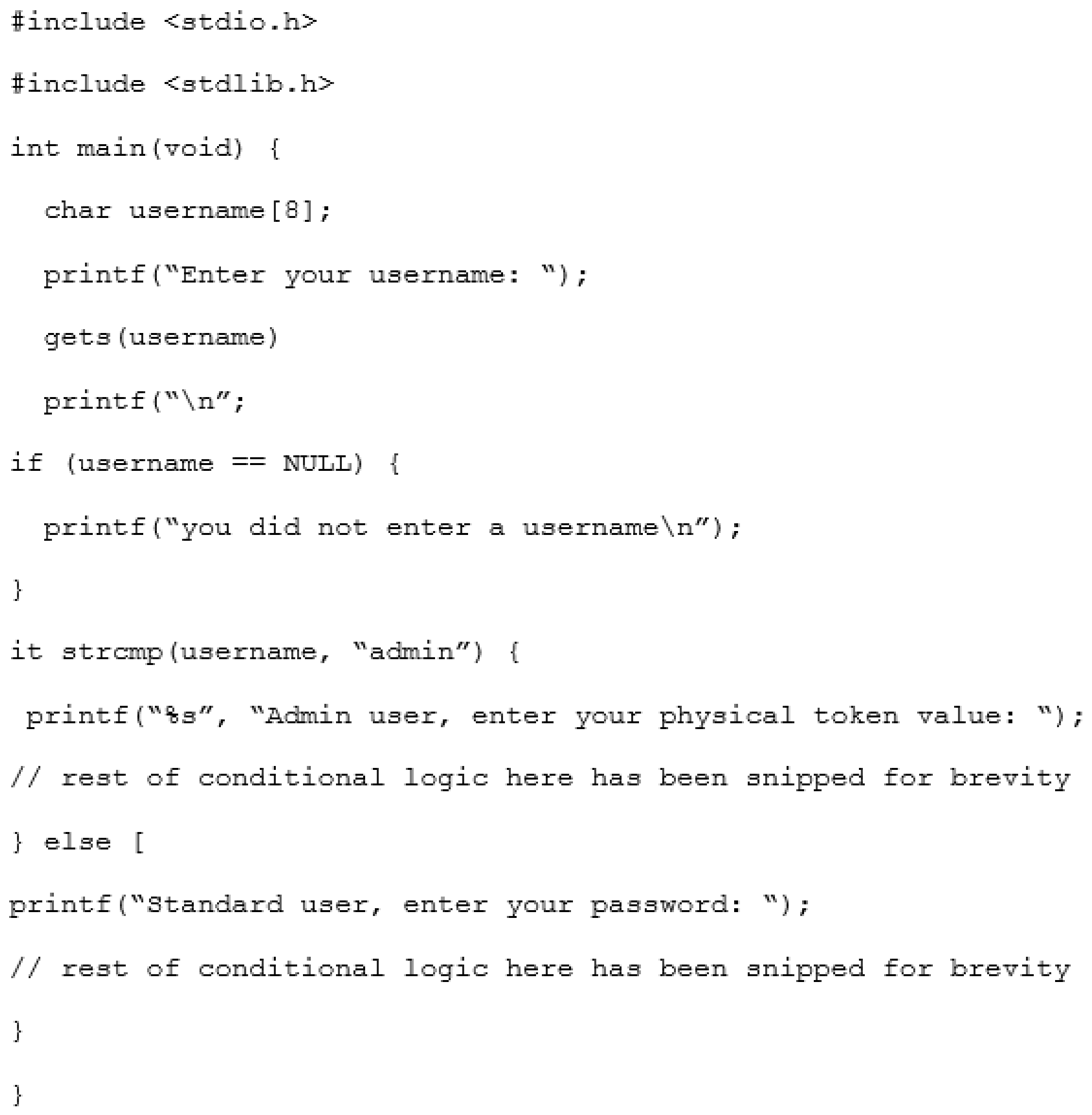
QUESTION 45
A company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

A. Use a protocol analyzer against the site to see if data input can be replayed from the browser
B. Scan the website through an interception proxy and identify areas for the code injection
C. Scan the site with a port scanner to identify vulnerable services running on the web server
D. Use network enumeration tools to identify if the server is running behind a load balancer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Given the code snippet below:



```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

  char username[8];

  printf(“Enter your username: “);

  gets(username)

  printf(“\n”;

if (username == NULL) {

  printf(“you did not enter a username\n”);

}

it strcmp(username, “admin”) {

 printf(“%s”, “Admin user, enter your physical token value: “);

// rest of conditional logic here has been snipped for brevity

} else [

printf(“Standard user, enter your password: “);

// rest of conditional logic here has been snipped for brevity

}

}
```

Which of the following vulnerability types in the MOST concerning?

A. Only short usernames are supported, which could result in brute forcing of credentials.
B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
C. Hardcoded usernames with different code paths taken depend on which user is entered.
D. Format string vulnerability is present for admin users but not for standard users.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
To meet an SLA, which of the following document should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

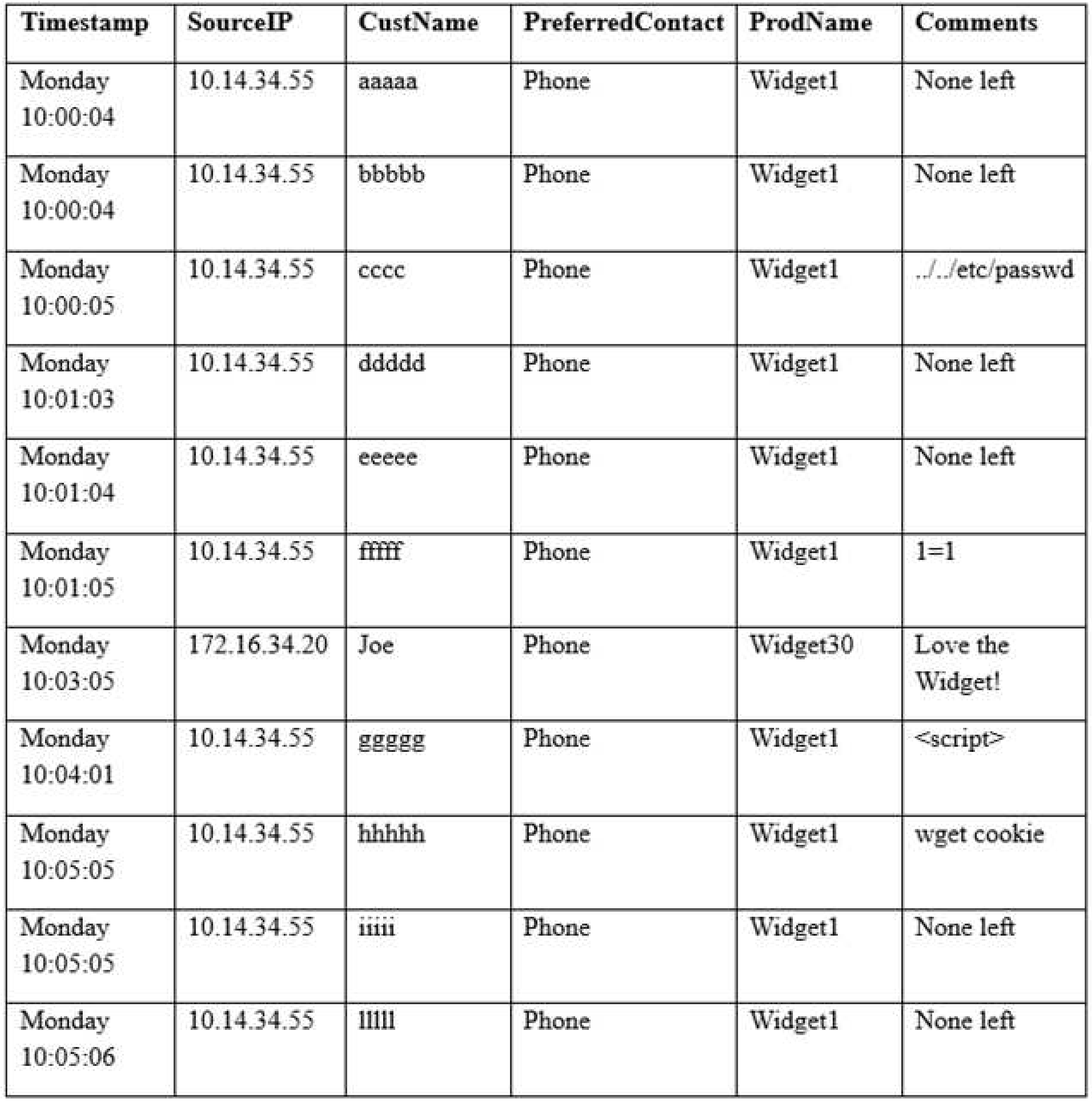
A. BPA
B. OLA
C. MSA
D. MOU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

QUESTION 48
A security analyst sees some suspicious entries in a log file from a web server website, which has a form that allows customers to leave feedback on the company's products. The analyst believes a malicious actor is scanning the web form. To know which security controls to put in place, the analyst first needs to determine the type of activity occurring to design a control. Given the log below:



Timestamp	SourceIP	CustName	PreferredContact	ProdName	Comments
Monday 10:00:04	10.14.34.55	aaaaa	Phone	Widget1	None left
Monday 10:00:04	10.14.34.55	bbbbb	Phone	Widget1	None left
Monday 10:00:05	10.14.34.55	cccc	Phone	Widget1	../../etc/passwd
Monday 10:01:03	10.14.34.55	ddddd	Phone	Widget1	None left
Monday 10:01:04	10.14.34.55	eeeee	Phone	Widget1	None left
Monday 10:01:05	10.14.34.55	fffff	Phone	Widget1	1=1
Monday 10:03:05	172.16.34.20	Joe	Phone	Widget30	Love the Widget!
Monday 10:04:01	10.14.34.55	ggggg	Phone	Widget1	<script>
Monday 10:05:05	10.14.34.55	hhhhh	Phone	Widget1	wget cookie
Monday 10:05:05	10.14.34.55	iiiii	Phone	Widget1	None left
Monday 10:05:06	10.14.34.55	lllll	Phone	Widget1	None left

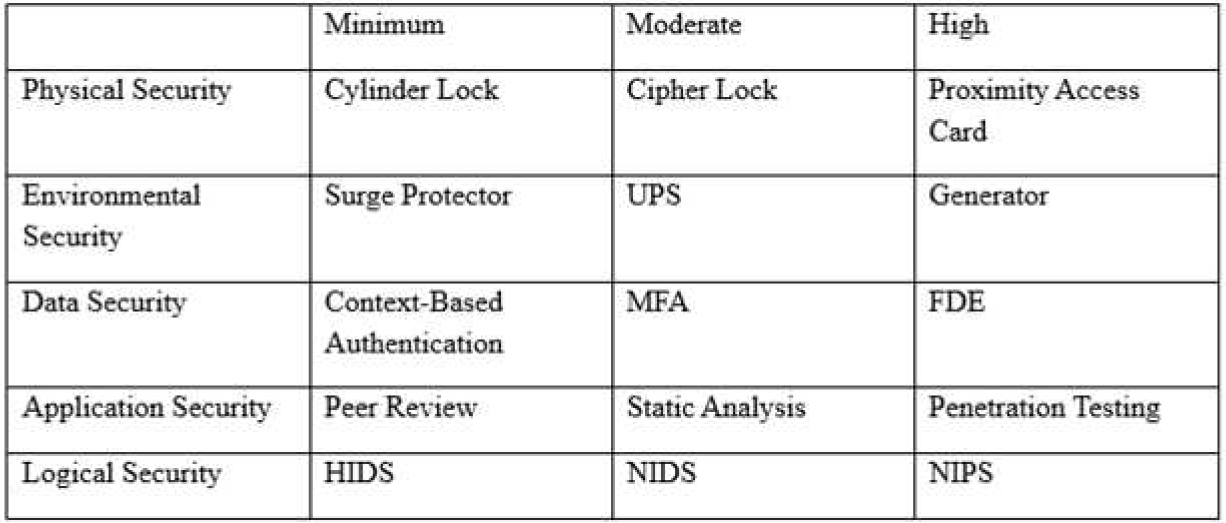
Which of the following is the MOST likely type of activity occurring?

A. SQL injection
B. XSS scanning
C. Fuzzing
D. Brute forcing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
An organization has established the following controls matrix:



	Minimum	Moderate	High
Physical Security	Cylinder Lock	Cipher Lock	Proximity Access Card
Environmental Security	Surge Protector	UPS	Generator
Data Security	Context-Based Authentication	MFA	FDE
Application Security	Peer Review	Static Analysis	Penetration Testing
Logical Security	HIDS	NIDS	NIPS

The following control sets have been defined by the organization and are applied in aggregate fashion:

- Systems containing PII are protected with the minimum control set.
- Systems containing medical data are protected at the moderate level.
- Systems containing cardholder data are protected at the high level.

The organization is preparing to deploy a system that protects the confidentially of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

A. Proximity card access to the server room, context-based authentication, UPS, and full-disk encryption for the database server.
B. Cipher lock on the server room door, FDE, surge protector, and static analysis of all application code.
C. Peer review of all application changes, static analysis of application code, UPS, and penetration testing of the complete system.
D. Intrusion detection capabilities, network-based IPS, generator, and context-based authentication.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Security policies that are in place at an organization prohibit USB drives from being utilized across the entire enterprise, with adequate technical controls in place to block them. As a way to still be able to work from various locations on different computing resources, several sales staff members have signed up for a web-based storage solution without the consent of the IT department. However, the operations department is required to use the same service to transmit certain business partner documents.

Which of the following would BEST allow the IT department to monitor and control this behavior?

A. Enabling AAA
B. Deploying a CASB
C. Configuring an NGFW
D. Installing a WAF
E. Utilizing a vTPM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Legal counsel has notified the information security manager of a legal matter that will require the preservation of electronic records for 2000 sales force employees.

Source records will be email, PC, network shares, and applications.

After all restrictions have been lifted, which of the following should the information manager review?

A. Data retention policy
B. Legal hold
C. Chain of custody
D. Scope statement

Correct Answer: A
Section: (none)
Explanation

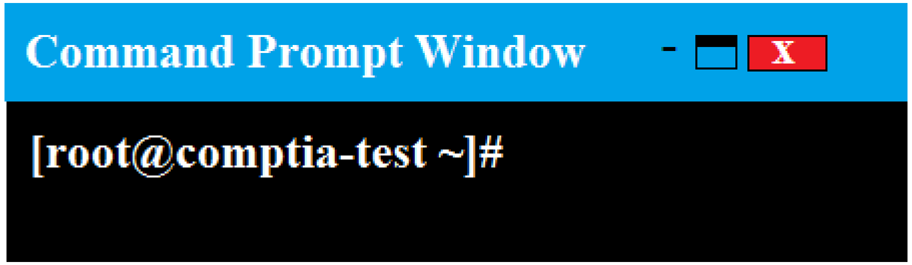
Explanation/Reference:

QUESTION 52
SIMULATION

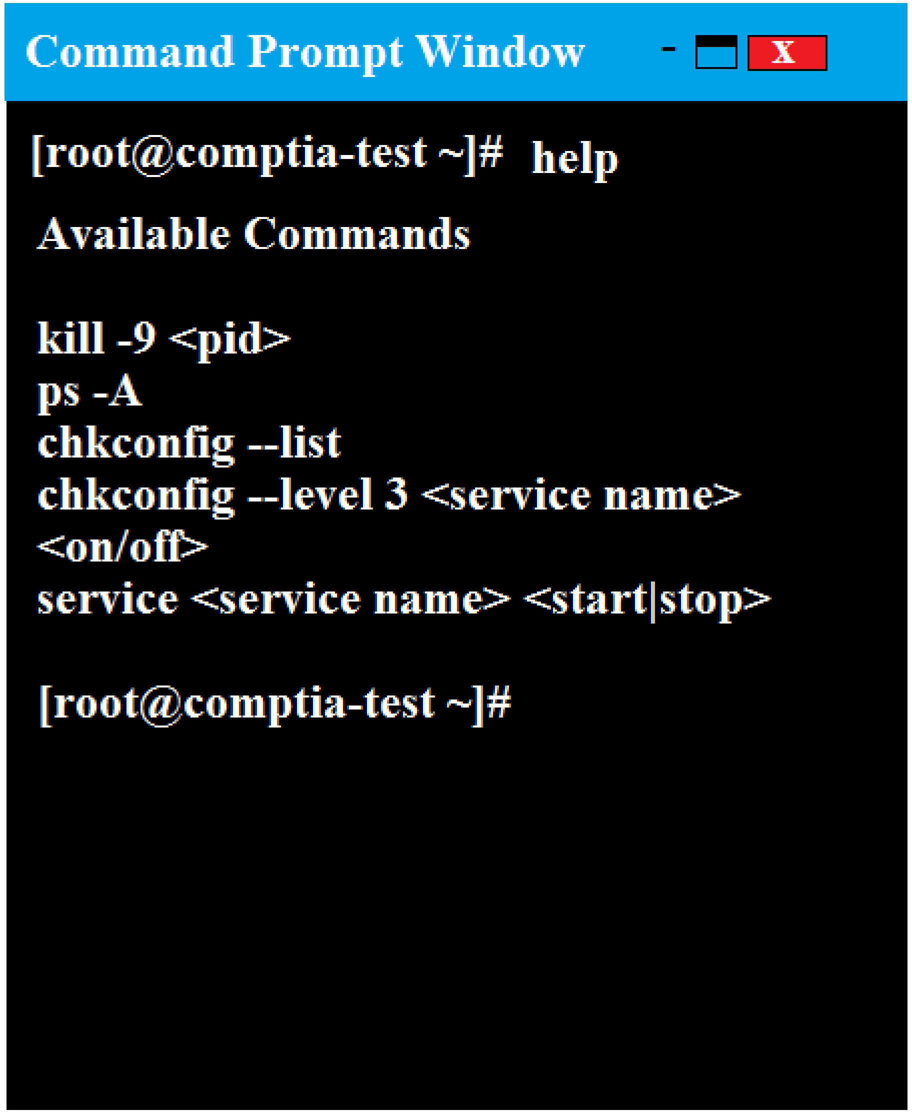
As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.
This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.
The command window will be provided along with root access. You are connected via a secure shell with root access.
You may query help for a list of commands.

Instructions:

You need to disable and turn off unrelated services and processes.
It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
[root@comptia-test ~]#
```



```
[root@comptia-test ~]#  help
Available Commands

kill -9 <pid>
ps -A
chkconfig --list
chkconfig --level 3 <service name>
<on/off>
service <service name> <start|stop>

[root@comptia-test ~]#
```

Correct Answer: See the explanation below
Section: (none)
Explanation

Explanation/Reference:

Explanation:

In Order to deactivate web services, database services and print service, we can do following things

1) deactivate its services

```
/etc/init.d/apache2 stop
/etc/init.d/mysqld stop
```

2) close ports for these services

Web Server

```
iptables -I INPUT -p tcp -m tcp --dport 443 -j REJECT
service iptables save
```

Print Server

```
iptables -I INPUT -p tcp -m tcp --dport 631 -j REJECT
service iptables save
```

Database Server

```
iptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECT
service iptables save
```

3) Kill the process any running for the same

```
ps -aef|grep mysql
kill -9 <<process id>>
```

QUESTION 53

The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloud-based log aggregation solution for all traffic that is logged.

Which of the following presents a long-term risk to user privacy in this scenario?

A. Confidential or sensitive documents are inspected by the firewall before being logged.

B. Latency when viewing videos and other online content may increase.

C. Reports generated from the firewall will take longer to produce due to more information from inspected traffic.

D. Stored logs may contain non-encrypted usernames and passwords for personal websites.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators.

Which of the following is MOST likely to produce the needed information?

A. Whois
B. DNS enumeration
C. Vulnerability scanner
D. Fingerprinting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources.

Which of the following should the analyst use to remediate the vulnerabilities?

A. Protocol analyzer
B. Root cause analysis
C. Behavioral analytics
D. Data leak prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

A. Effective deployment of network taps

B. Overall bandwidth available at Internet PoP
C. Optimal placement of log aggregators
D. Availability of application layer visualizers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an exploit.

Which of the following would provide greater insight on the potential impact of this attempted attack?

A. Run an antivirus scan on the finance PC.
B. Use a protocol analyzer on the air-gapped PC.
C. Perform reverse engineering on the document.
D. Analyze network logs for unusual traffic.
E. Run a baseline analyzer against the user’s computer.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials.

Which of the following tools should be used? (Choose two.)

A. Fuzzer
B. SCAP scanner

C. Packet analyzer
D. Password cracker
E. Network enumerator
F. SIEM

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points.

Which of the following solutions BEST meets the engineer's goal?

A. Schedule weekly reviews of al unit test results with the entire development team and follow up between meetings with surprise code inspections.
B. Develop and implement a set of automated security tests to be installed on each development team leader's workstation.
C. Enforce code quality and reuse standards into the requirements definition phase of the waterfall development process.
D. Deploy an integrated software tool that builds and tests each portion of code committed by developers and provides feedback.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers.

Which of the following BEST describes the contents of the supporting document the engineer is creating?

A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.
B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.
C. A set of formal methods that apply to one or more of the programing languages used on the development project.
D. A methodology to verify each security control in each unit of developed code prior to committing the code.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A security technician is incorporating the following requirements in an RFP for a new SIEM:

- New security notifications must be dynamically implemented by the SIEM engine
- The SIEM must be able to identify traffic baseline anomalies
- Anonymous attack data from all customers must augment attack detection and risk scoring

Based on the above requirements, which of the following should the SIEM support? (Choose two.)

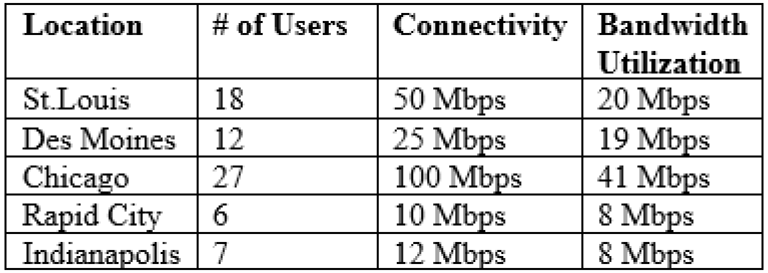
A. Autoscaling search capability
B. Machine learning
C. Multisensor deployment
D. Big Data analytics
E. Cloud-based management
F. Centralized log aggregation

Correct Answer: BD
Section: (none)
Explanation

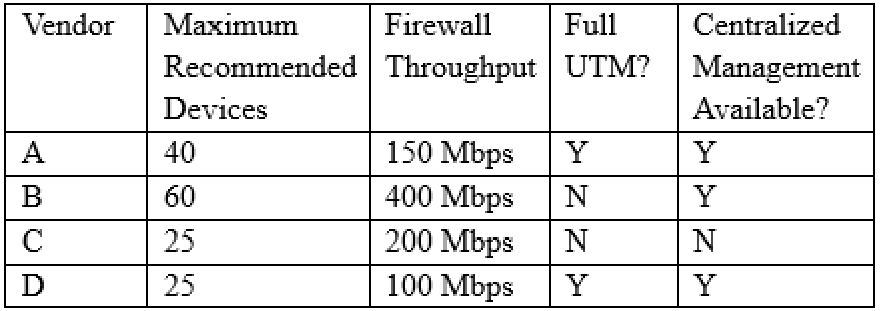
Explanation/Reference:

QUESTION 62
Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the requirements that it be easy to manage and provide capacity for growth.

The tables below provide information on a subset of remote sites and the firewall options:



Location	# of Users	Connectivity	Bandwidth Utilization
St.Louis	18	50 Mbps	20 Mbps
Des Moines	12	25 Mbps	19 Mbps
Chicago	27	100 Mbps	41 Mbps
Rapid City	6	10 Mbps	8 Mbps
Indianapolis	7	12 Mbps	8 Mbps



Vendor	Maximum Recommended Devices	Firewall Throughput	Full UTM?	Centralized Management Available?
A	40	150 Mbps	Y	Y
B	60	400 Mbps	N	Y
C	25	200 Mbps	N	N
D	25	100 Mbps	Y	Y

Which of the following would be the BEST option to recommend to the CIO?

A. Vendor C for small remote sites, and Vendor B for large sites.
B. Vendor B for all remote sites
C. Vendor C for all remote sites
D. Vendor A for all remote sites
E. Vendor D for all remote sites

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

- Involve business owners and stakeholders
- Create an applicable scenario
- Conduct a biannual verbal review of the incident response plan
- Report on the lessons learned and gaps identified

Which of the following exercises has the CEO requested?

A. Parallel operations

B. Full transition

C. Internal review

D. Tabletop

E. Partial simulation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?

A. Check for any relevant or required overlays.

B. Review enhancements within the current control set.

C. Modify to a high-baseline set of controls.

D. Perform continuous monitoring.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A security researcher is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

Based on the information available to the researcher, which of the following is the MOST likely threat profile?

A. Nation-state-sponsored attackers conducting espionage for strategic gain.
B. Insiders seeking to gain access to funds for illicit purposes.
C. Opportunists seeking notoriety and fame for personal gain.
D. Hacktivists seeking to make a political statement because of socio-economic factors.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A security analyst is inspecting pseudocode of the following multithreaded application:

```
1. perform daily ETL of data
1.1 validate that yesterday’s data model file exists
1.2 validate that today’s data model file does not exist
1.2 extract yesterday’s data model
1.3 transform the format
1.4 load the transformed data into today’s data model file
1.5 exit
```

Which of the following security concerns is evident in the above pseudocode?

A. Time of check/time of use
B. Resource exhaustion
C. Improper storage of sensitive data
D. Privilege escalation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations.

Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

A. Malicious insiders will not have the opportunity to tamper with data at rest and affect the integrity of the system.
B. Thin client workstations require much less security because they lack storage and peripherals that can be easily compromised, and the virtual workstations are protected in the cloud where security is outsourced.
C. All thin clients use TPM for core protection, and virtual workstations use vTPM for core protection with both equally ensuring a greater security advantage for a cloud-hosted environment.
D. Malicious users will have reduced opportunities for data extractions from their physical thin client workstations, this reducing the effectiveness of local attacks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use.

After network enumeration, the analyst's NEXT step is to perform:

A. a gray-box penetration test
B. a risk analysis
C. a vulnerability assessment
D. an external security audit
E. a red team exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:

1. Information should be sourced from the trusted master data source.
2. There must be future requirements for identity proofing of devices and users.
3. A generic identity connector that can be reused must be developed.
4. The current project scope is for internally hosted applications only.

Which of the following solution building blocks should the security architect use to BEST meet the requirements?

A. LDAP, multifactor authentication, oAuth, XACML
B. AD, certificate-based authentication, Kerberos, SPML
C. SAML, context-aware authentication, oAuth, WAYF
D. NAC, radius, 802.1x, centralized active directory

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

A. Lack of adequate in-house testing skills.
B. Requirements for geographically based assessments
C. Cost reduction measures
D. Regulatory insistence on independent reviews.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: non-sensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive.

Which of the following actions should the engineer take regarding the data?

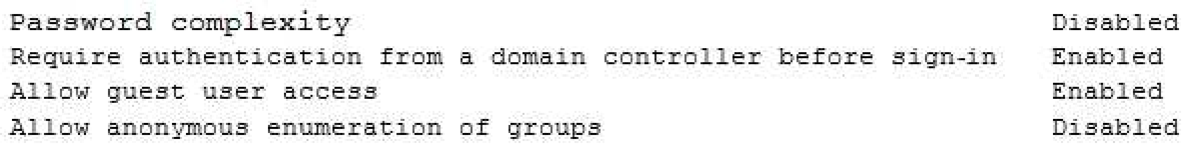
A. Label the data as extremely sensitive.
B. Label the data as sensitive but accessible.
C. Label the data as non-sensitive.
D. Label the data as sensitive but export-controlled.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:

Which of the following tools is the engineer utilizing to perform this assessment?



```
Password complexity                                           Disabled
Require authentication from a domain controller before sign-in   Enabled
Allow guest user access                                       Enabled
Allow anonymous enumeration of groups                         Disabled
```

A. Vulnerability scanner
B. SCAP scanner

C. Port scanner
D. Interception proxy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues.

Which of the following is the MOST important information to reference in the letter?

A. After-action reports from prior incidents.
B. Social engineering techniques
C. Company policies and employee NDAs
D. Data classification processes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A database administrator is required to adhere to and implement privacy principles when executing daily tasks. A manager directs the administrator to reduce the number of unique instances of PII stored within an organization’s systems to the greatest extent possible.

Which of the following principles is being demonstrated?

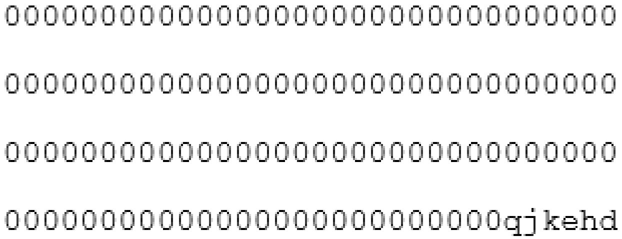
A. Administrator accountability
B. PII security
C. Record transparency
D. Data minimization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.

To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:



```
00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000qjkehd
```

Which of the following should be included in the auditor’s report based on the above findings?

A. The hard disk contains bad sectors
B. The disk has been degaussed.
C. The data represents part of the disk BIOS.
D. Sensitive data might still be present on the hard drives.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other users’ emails. Review of a tool’s

output shows the administrators have used web mail to log into other users’ inboxes.

Which of the following tools would show this type of output?

A. Log analysis tool
B. Password cracker
C. Command-line tool
D. File integrity monitoring tool

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:

Configuration file 1:

```
Operator ALL=/sbin/reboot
```

Configuration file 2:

```
Command=”/sbin/shutdown now”, no-x11-forwarding, no-pty, ssh-dss
```

Configuration file 3:

```
Operator:x:1000:1000::/home/operator:/bin/bash
```

Which of the following explains why an intended operator cannot perform the intended action?

A. The sudoers file is locked down to an incorrect command
B. SSH command shell restrictions are misconfigured
C. The passwd file is misconfigured
D. The SSH command is not allowing a pty session

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured.

A stand up has identified the following additional requirements:

1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications

Which of the following solution components should be deployed to BEST meet the requirements? (Select three.)

A. IPSec VPN
B. HIDS
C. Wireless controller
D. Rights management
E. SSL VPN
F. NAC
G. WAF
H. Load balancer

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.

Which of the following solutions BEST meets all of the architect's objectives?

A. An internal key infrastructure that allows users to digitally sign transaction logs
B. An agreement with an entropy-as-a-service provider to increase the amount of randomness in generated keys.

C. A publicly verified hashing algorithm that allows revalidation of message integrity at a future date.
D. An open distributed transaction ledger that requires proof of work to append entries.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A user asks a security practitioner for recommendations on securing a home network. The user recently purchased a connected home assistant and multiple IoT devices in an effort to automate the home. Some of the IoT devices are wearables, and other are installed in the user's automobiles. The current home network is configured as a single flat network behind an ISP-supplied router. The router has a single IP address, and the router performs NAT on incoming traffic to route it to individual devices.

Which of the following security controls would address the user's privacy concerns and provide the BEST level of security for the home network?

A. Ensure all IoT devices are configured in a geofencing mode so the devices do not work when removed from the home network. Disable the home assistant unless actively using it, and segment the network so each IoT device has its own segment.
B. Install a firewall capable of cryptographically separating network traffic, require strong authentication to access all IoT devices, and restrict network access for the home assistant based on time-of-day restrictions.
C. Segment the home network to separate network traffic from users and the IoT devices, ensure security settings on the home assistant support no or limited recording capability, and install firewall rules on the router to restrict traffic to the home assistant as much as possible.
D. Change all default passwords on the IoT devices, disable Internet access for the IoT devices and the home assistant, obtain routable IP addresses for all devices, and implement IPv6 and IPSec protections on all network traffic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES-256-GCM on VPNs between sites.

Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

A. Add a second-layer VPN from a different vendor between sites.
B. Upgrade the cipher suite to use an authenticated AES mode of operation.
C. Use a stronger elliptic curve cryptography algorithm.
D. Implement an IDS with sensors inside (clear-text) and outside (cipher-text) of each tunnel between sites.
E. Ensure cryptography modules are kept up to date from vendor supplying them.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
The government is concerned with remote military missions being negatively being impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:

- End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.
- Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications
- A host-based whitelist of approved websites and applications that only allow mission-related tools and sites
- The use of satellite communication to include multiple proxy servers to scramble the source IP address

Which of the following is of MOST concern in this scenario?

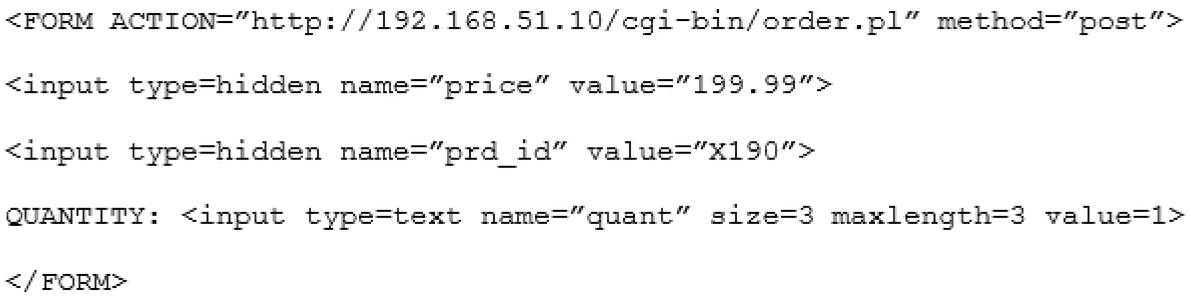
A. Malicious actors intercepting inbound and outbound communication to determine the scope of the mission
B. Family members posting geotagged images on social media that were received via email from soldiers
C. The effect of communication latency that may negatively impact real-time communication with mission control
D. The use of centrally managed military network and computers by soldiers when communicating with external parties

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83

Given the following code snippet:



```
<FORM ACTION=”http://192.168.51.10/cgi-bin/order.pl” method=”post”>

<input type=hidden name=”price” value=”199.99”>

<input type=hidden name=”prd_id” value=”X190”>

QUANTITY: <input type=text name=”quant” size=3 maxlength=3 value=1>

</FORM>
```

Of which of the following is this snippet an example?

A. Data execution prevention
B. Buffer overflow
C. Failure to use standard libraries
D. Improper filed usage
E. Input validation

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
A company has created a policy to allow employees to use their personally owned devices. The Chief Information Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices.

Which of the following security controls would BEST reduce the risk of exposure?

A. Disk encryption on the local drive
B. Group policy to enforce failed login lockout
C. Multifactor authentication
D. Implementation of email digital signatures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
After a large organization has completed the acquisition of a smaller company, the smaller company must implement new host-based security controls to connect its employees' devices to the network. Given that the network requires 802.1X EAP-PEAP to identify and authenticate devices, which of the following should the security administrator do to integrate the new employees' devices into the network securely?

A. Distribute a NAC client and use the client to push the company's private key to all the new devices.
B. Distribute the device connection policy and a unique public/private key pair to each new employee's device.
C. Install a self-signed SSL certificate on the company's RADIUS server and distribute the certificate's public key to all new client devices.
D. Install an 802.1X supplicant on all new devices and let each device generate a self-signed certificate to use for network access.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:

```
dd if=/dev/ram of=/tmp/mem/dmp
```

The analyst then reviews the associated output:

```
^34^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/bin/bash^21^03#45
```

However, the analyst is unable to find any evidence of the running shell.

Which of the following of the MOST likely reason the analyst cannot find a process ID for the shell?

A. The NX bit is enabled
B. The system uses ASLR
C. The shell is obfuscated
D. The code uses dynamic libraries

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back.

Which of the following BEST describes how the manager should respond?

A. Determine if the data still exists by inspecting to ascertain if the laptop has already been wiped and if the storage team has recent backups.
B. Inform Ann that the laptop was for company data only and she should not have stored personal photos on a company asset.
C. Report the email because it may have been a spoofed request coming from an attacker who is trying to exfiltrate data from the company laptop.
D. Consult with the legal and/or human resources department and check company policies around employment and termination procedures.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently. All paper records are scheduled to be shredded in a crosscut shredded, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.

Which of the following would ensure no data is recovered from the system drives once they are disposed of?

A. Overwriting all HDD blocks with an alternating series of data.
B. Physically disabling the HDDs by removing the dive head.
C. Demagnetizing the hard drive using a degausser.
D. Deleting the UEFI boot loaders from each HDD.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A company has decided to lower costs by conducting an internal assessment on specific devices and various internal and external subnets. The assessment will be done during regular office hours, but it must not affect any production servers.

Which of the following would MOST likely be used to complete the assessment? (Select two.)

A. Agent-based vulnerability scan
B. Black-box penetration testing
C. Configuration review
D. Social engineering
E. Malware sandboxing
F. Tabletop exercise

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.

Which of the following is the BEST solution?

A. Use an entropy-as-a-service vendor to leverage larger entropy pools.
B. Loop multiple pseudo-random number generators in a series to produce larger numbers.
C. Increase key length by two orders of magnitude to detect brute forcing.
D. Shift key generation algorithms to ECC algorithms.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

A. Making employees rotate through jobs ensures succession plans can be implemented and prevents single point of failure.
B. Forcing different people to perform the same job minimizes the amount of time malicious actions go undetected by forcing malicious actors to attempt collusion between two or more people.
C. Administrators and engineers who perform multiple job functions throughout the day benefit from being cross-trained in new job areas.
D. It eliminates the need to share administrative account passwords because employees gain administrative rights as they rotate into a new job area.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.

Which of the following is the MOST appropriate order of steps to be taken?

A. Firmware update, OS patching, HIDS, antivirus, baseline, monitoring agent
B. OS patching, baseline, HIDS, antivirus, monitoring agent, firmware update
C. Firmware update, OS patching, HIDS, antivirus, monitoring agent, baseline
D. Baseline, antivirus, OS patching, monitoring agent, HIDS, firmware update

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the

organization plan to leverage?

A. SaaS
B. PaaS
C. IaaS
D. Hybrid cloud
E. Network virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

A. Code repositories
B. Security requirements traceability matrix
C. Software development lifecycle
D. Data design diagram
E. Roles matrix
F. Implementation guide

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

A. Port security
B. Rogue device detection
C. Bluetooth
D. GPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

A. Reconfigure the firewall to block external UDP traffic.
B. Establish a security baseline on the IDS.
C. Block echo reply traffic at the firewall.
D. Modify the edge router to not forward broadcast traffic.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
An administrator is working with management to develop policies related to the use of the cloud-based resources that contain corporate data. Management plans to require some control over organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management’s policy?

A. MDM
B. Sandboxing
C. Mobile tokenization
D. FDE
E. MFA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Users have been reporting unusual automated phone calls, including names and phone numbers, that appear to come from devices internal to the company. Which of the following should the systems administrator do to BEST address this problem?

A. Add an ACL to the firewall to block VoIP.
B. Change the settings on the phone system to use SIP-TLS.
C. Have the phones download new configurations over TFTP.
D. Enable QoS configuration on the phone VLAN.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:

```
TCP 80 open
TCP 443 open
TCP 1434 filtered
```

The penetration tester then used a different tool to make the following requests:

```
GET / script/login.php?token=45$MHT000MND876
GET / script/login.php?token=@#984DCSPQ%091DF
```

Which of the following tools did the penetration tester use?

A. Protocol analyzer
B. Port scanner

C. Fuzzer
D. Brute forcer
E. Log analyzer
F. HTTP interceptor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

A. Summarize the most recently disclosed vulnerabilities.
B. Research industry best practices and latest RFCs.
C. Undertake an external vulnerability scan and penetration test.
D. Conduct a threat modeling exercise.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This vulnerability does not significantly expose the enterprise to risk and would be expensive against.

Which of the following strategies should the engineer recommended be approved FIRST?

A. Avoid

B. Mitigate
C. Transfer
D. Accept

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle.

Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

A. Install and configure an IPS.
B. Enforce routine GPO reviews.
C. Form and deploy a hunt team.
D. Institute heuristic anomaly detection.
E. Use a protocol analyzer with appropriate connectors.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A security engineer is deploying an IdP to broker authentication between applications. These applications all utilize SAML 2.0 for authentication. Users log into the IdP with their credentials and are given a list of applications they may access. One of the application's authentications is not functional when a user initiates an authentication attempt from the IdP. The engineer modifies the configuration so users browse to the application first, which corrects the issue. Which of the following BEST describes the root cause?

A. The application only supports SP-initiated authentication.
B. The IdP only supports SAML 1.0
C. There is an SSL certificate mismatch between the IdP and the SaaS application.

D. The user is not provisioned correctly on the IdP.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A security manager recently categorized an information system. During the categorization effort, the manager determined the loss of integrity of a specific information type would impact business significantly. Based on this, the security manager recommends the implementation of several solutions. Which of the following, when combined, would BEST mitigate this risk? (Select TWO.)

A. Access control
B. Whitelisting
C. Signing
D. Validation
E. Boot attestation

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
After several industry comnpetitors suffered data loss as a result of cyebrattacks, the Chief Operating Officer (COO) of a company reached out to the information security manager to review the organization's security stance. As a result of the discussion, the COO wants the organization to meet the following criteria:

- Blocking of suspicious websites
- Prevention of attacks based on threat intelligence
- Reduction in spam
- Identity-based reporting to meet regulatory compliance
- Prevention of viruses based on signature
- Protect applications from web-based threats

Which of the following would be the BEST recommendation the information security manager could make?

A. Reconfigure existing IPS resources
B. Implement a WAF
C. Deploy a SIEM solution
D. Deploy a UTM solution
E. Implement an EDR platform

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
A company's chief cybersecurity architect wants to configure mutual authentication to access an internal payroll website. The architect has asked the administration team to determine the configuration that would provide the best defense against MITM attacks. Which of the following implementation approaches would BEST support the architect's goals?

A. Utilize a challenge-response prompt as required input at username/password entry.
B. Implement TLS and require the client to use its own certificate during handshake.
C. Configure a web application proxy and institute monitoring of HTTPS transactions.
D. Install a reverse proxy in the corporate DMZ configured to decrypt TLS sessions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A company is not familiar with the risks associated with IPv6. The systems administrator wants to isolate IPv4 from IPv6 traffic between two different network segments. Which of the following should the company implement? (Select TWO)

A. Use an internal firewall to block UDP port 3544.
B. Disable network discovery protocol on all company routers.
C. Block IP protocol 41 using Layer 3 switches.
D. Disable the DHCPv6 service from all routers.

E. Drop traffic for ::/0 at the edge firewall.
F. Implement a 6in4 proxy server.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
With which of the following departments should an engineer for a consulting firm coordinate when determining the control and reporting requirements for storage of sensitive, proprietary customer information?

A. Human resources
B. Financial
C. Sales
D. Legal counsel

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
The Chief Executive Officers (CEOs) from two different companies are discussing the highly sensitive prospect of merging their respective companies together. Both have invited their Chief Information Officers (CIOs) to discern how they can securely and digitally communicate, and the following criteria are collectively determined:

- Must be encrypted on the email servers and clients
- Must be OK to transmit over unsecure Internet connections

Which of the following communication methods would be BEST to recommend?

A. Force TLS between domains.
B. Enable STARTTLS on both domains.
C. Use PGP-encrypted emails.

D. Switch both domains to utilize DNSSEC.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A bank is initiating the process of acquiring another smaller bank. Before negotiations happen between the organizations, which of the following business documents would be used as the FIRST step in the process?

A. MOU
B. OLA
C. BPA
D. NDA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A company wants to confirm sufficient executable space protection is in place for scenarios in which malware may be attempting buffer overflow attacks. Which of the following should the security engineer check?

A. NX/XN
B. ASLR
C. strcpy
D. ECC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in secure environment?

A. NDA
B. MOU
C. BIA
D. SLA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

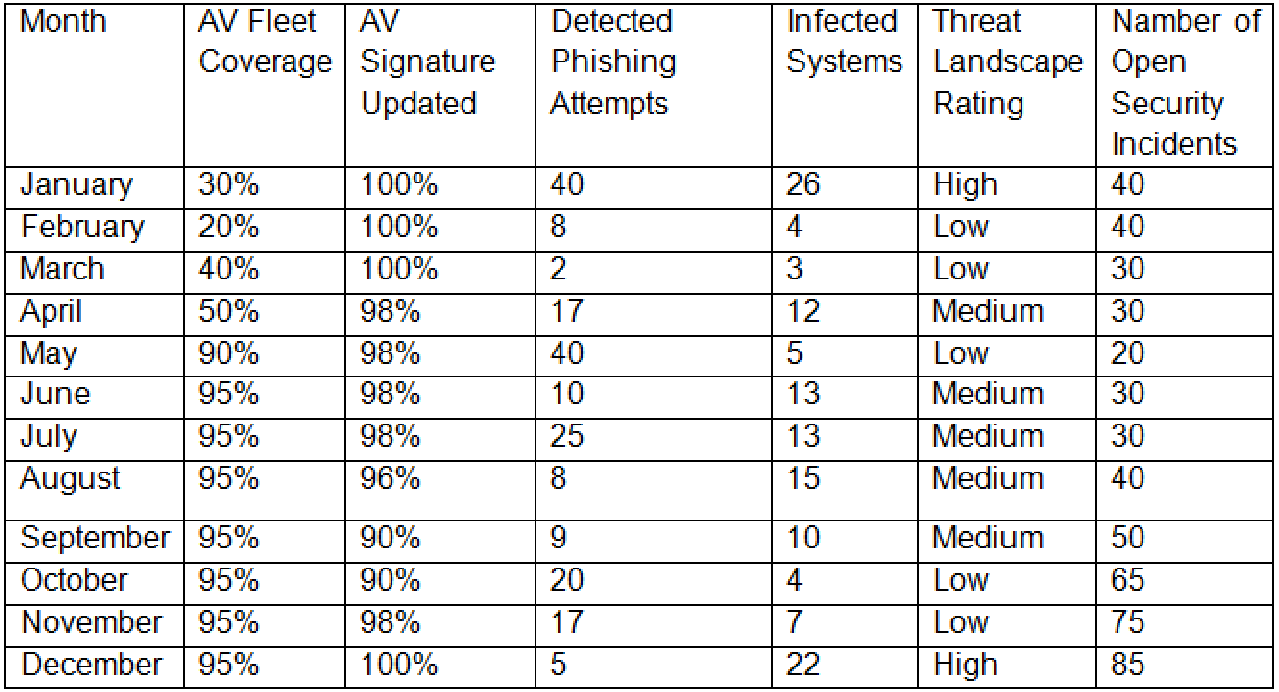
QUESTION 113
Developers are working on anew feature to add to a social media platform. Thew new feature involves users uploading pictures of what they are currently doing. The data privacy officer (DPO) is concerned about various types of abuse that might occur due to this new feature. The DPO state the new feature cannot be released without addressing the physical safety concerns of the platform's users. Which of the following controls would BEST address the DPO's concerns?

A. Increasing blocking options available to the uploader
B. Adding a one-hour delay of all uploaded photos
C. Removing all metadata in the uploaded photo file
D. Not displaying to the public who uploaded the photo
E. Forcing TLS for all connections on the platform

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
A security technician receives a copy of a report that was originally sent to the board of directors by the Chief Information Security Officer (CISO).
The report outlines the following KPI/KRI data for the last 12 months:



Month	AV Fleet Coverage	AV Signature Updated	Detected Phishing Attempts	Infected Systems	Threat Landscape Rating	Namber of Open Security Incidents
January	30%	100%	40	26	High	40
February	20%	100%	8	4	Low	40
March	40%	100%	2	3	Low	30
April	50%	98%	17	12	Medium	30
May	90%	98%	40	5	Low	20
June	95%	98%	10	13	Medium	30
July	95%	98%	25	13	Medium	30
August	95%	96%	8	15	Medium	40
September	95%	90%	9	10	Medium	50
October	95%	90%	20	4	Low	65
November	95%	98%	17	7	Low	75
December	95%	100%	5	22	High	85

Which of the following BEST describes what could be interpreted from the above data?

A. 1. AV coverage across the fleet improved
2. There is no correlation between infected systems and AV coverage.
3. There is no correlation between detected phishing attempts and infected systems
4. A correlation between threat landscape rating and infected systems appears to exist.
5. Effectiveness and performance of the security team appears to be degrading.

B. 1. AV signature coverage has remained consistently high
2. AV coverage across the fleet improved
3. A correlation between phishing attempts and infected systems appears to exist
4. There is a correlation between the threat landscape rating and the security team’s performance.
5. There is no correlation between detected phishing attempts and infected systems

C. 1. There is no correlation between infected systems and AV coverage
2. AV coverage across the fleet improved
3. A correlation between phishing attempts and infected systems appears to exist
4. There is no correlation between the threat landscape rating and the security team’s performance.

5. There is a correlation between detected phishing attempts and infected systems

D. 1. AV coverage across the fleet declined
   2. There is no correlation between infected systems and AV coverage.
   3. A correlation between phishing attempts and infected systems appears to exist
   4. There is no correlation between the threat landscape rating and the security team's performance
   5. Effectiveness and performance of the security team appears to be degrading.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
A Chief Information Security Officer (CISO) is reviewing the controls in place to support the organization's vulnerability management program. The CISO finds patching and vulnerability scanning policies and procedures are in place. However, the CISO is concerned the organization is siloed and is not maintaining awareness of new risks to the organization. The CISO determines systems administrators need to participate in industry security events. Which of the following is the CISO looking to improve?

A. Vendor diversification
B. System hardening standards
C. Bounty programs
D. Threat awareness
E. Vulnerability signatures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
An organization is improving its web services to enable better customer engagement and self-service. The organization has a native mobile application and a rewards portal provided by a third party. The business wants to provide customers with the ability to log in once and have SSO between each of the applications. The integrity of the identity is important so it can be propagated through to back-end systems to maintain a consistent audit trail. Which of the following authentication and authorization types BEST meet the requirements? (Choose two.)

A. SAML

B. Social login
C. OpenID connect
D. XACML
E. SPML
F. OAuth

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
After the departure of a developer under unpleasant circumstances, the company is concerned about the security of the software to which the developer has access. Which of the following is the BEST way to ensure security of the code following the incident?

A. Hire an external red team to conduct black box testing
B. Conduct a peer review and cross reference the SRTM
C. Perform white-box testing on all impacted finished products
D. Perform regression testing and search for suspicious code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A software company is releasing a new mobile application to a broad set of external customers. Because the software company is rapidly releasing new features, it has built in an over-the-air software update process that can automatically update the application at launch time. Which of the following security controls should be recommended by the company's security architect to protect the integrity of the update process? (Choose two.)

A. Validate cryptographic signatures applied to software updates
B. Perform certificate pinning of the associated code signing key
C. Require HTTPS connections for downloads of software updates
D. Ensure there are multiple download mirrors for availability

E. Enforce a click-through process with user opt-in for new features

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
A Chief Information Security Officer (CISO) is developing a new BIA for the organization. The CISO wants to gather requirements to determine the appropriate RTO and RPO for the organization’s ERP. Which of the following should the CISO interview as MOST qualified to provide RTO/RPO metrics?

A. Data custodian
B. Data owner
C. Security analyst
D. Business unit director
E. Chief Executive Officer (CEO)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
A Chief Information Security Officer (CISO) requests the following external hosted services be scanned for malware, unsecured PII, and healthcare data:

- Corporate intranet site
- Online storage application
- Email and collaboration suite

Security policy also is updated to allow the security team to scan and detect any bulk downloads of corporate data from the company’s intranet and online storage site. Which of the following is needed to comply with the corporate security policy and the CISO’s request?

A. Port scanner
B. CASB
C. DLP agent
D. Application sandbox

E. SCAP scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
Several recent ransomware outbreaks at a company have cost a significant amount of lost revenue. The security team needs to find a technical control mechanism that will meet the following requirements and aid in preventing these outbreaks:

- Stop malicious software that does not match a signature
- Report on instances of suspicious behavior
- Protect from previously unknown threats
- Augment existing security capabilities

Which of the following tools would BEST meet these requirements?

A. Host-based firewall

B. EDR

C. HIPS

D. Patch management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
A company that has been breached multiple times is looking to protect cardholder data. The previous undetected attacks all mimicked normal administrative-type behavior. The company must deploy a host solution to meet the following requirements:

- Detect administrative actions
- Block unwanted MD5 hashes
- Provide alerts
- Stop exfiltration of cardholder data

Which of the following solutions would BEST meet these requirements? (Choose two.)

A. AV
B. EDR
C. HIDS
D. DLP
E. HIPS
F. EFS

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

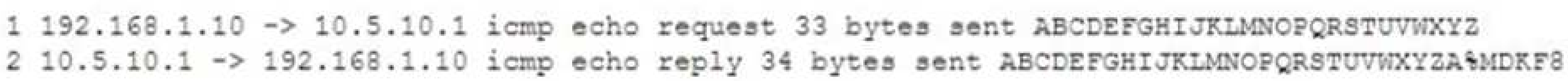
QUESTION 123
A security engineer is employed by a hospital that was recently purchased by a corporation. Throughout the acquisition process, all data on the virtualized file servers must be shared by departments within both organizations. The security engineer considers data ownership to determine:

A. the amount of data to be moved.
B. the frequency of data backups.
C. which users will have access to which data
D. when the file server will be decommissioned

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A security analyst is reviewing the following packet capture of communication between a host and a company's router:



```
1 192.168.1.10 -> 10.5.10.1 icmp echo request 33 bytes sent ABCDEFGHIJKLMNOPQRSTUVWXYZ
2 10.5.10.1 -> 192.168.1.10 icmp echo reply 34 bytes sent ABCDEFGHIJKLMNOPQRSTUVWXYZA%MDKF8
```

Which of the following actions should the security analyst take to remove this vulnerability?

A. Update the router code
B. Implement a router ACL
C. Disconnect the host from the network
D. Install the latest antivirus definitions
E. Deploy a network-based IPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A development team is testing an in-house-developed application for bugs. During the test, the application crashes several times due to null pointer exceptions. Which of the following tools, if integrated into an IDE during coding, would identify these bugs routinely?

A. Issue tracker
B. Static code analyzer
C. Source code repository
D. Fuzzing utility

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126

A systems administrator receives an advisory email that a recently discovered exploit is being used in another country and the financial institutions have ceased operations while they find a way to respond to the attack. Which of the following BEST describes where the administrator should look to find information on the attack to determine if a response must be prepared for the systems? (Choose two.)

A. Bug bounty websites
B. Hacker forums
C. Antivirus vendor websites
D. Trade industry association websites
E. CVE database
F. Company’s legal department

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A security assessor is working with an organization to review the policies and procedures associated with managing the organization’s virtual infrastructure. During a review of the virtual environment, the assessor determines the organization is using servers to provide more than one primary function, which violates a regulatory requirement. The assessor reviews hardening guides and determines policy allows for this configuration. It would be MOST appropriate for the assessor to advise the organization to:

A. segment dual-purpose systems on a hardened network segment with no external access
B. assess the risks associated with accepting non-compliance with regulatory requirements
C. update system implementation procedures to comply with regulations
D. review regulatory requirements and implement new policies on any newly provisioned servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
While conducting a BIA for a proposed acquisition, the IT integration team found that both companies outsource CRM services to competing and incompatible third-party cloud services. The decision has been made to bring the CRM service in-house, and the IT team has chosen a future solution. With which of the following

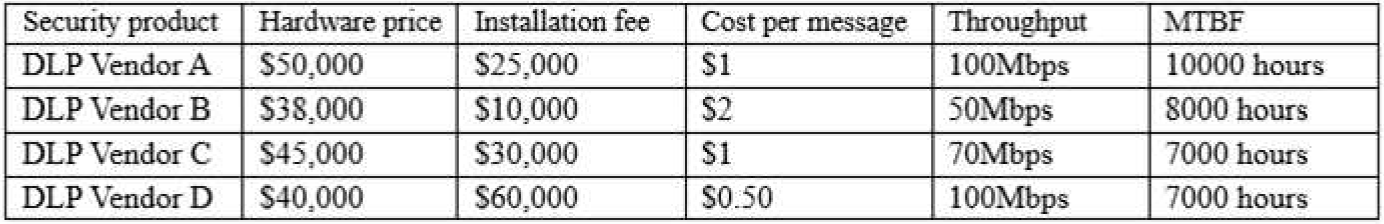
should the Chief Information Security Officer (CISO) be MOST concerned? (Choose two.)

A. Data remnants
B. Sovereignty
C. Compatible services
D. Storage encryption
E. Data migration
F. Chain of custody

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
A newly hired Chief Information Security Officer (CISO) is reviewing the organization’s security budget from the previous year. The CISO notices $100,000 worth of fines were paid for not properly encrypting outbound email messages. The CISO expects next year’s costs associated with fines to double and the volume of messages to increase by 100%. The organization sent out approximately 25,000 messages per year over the last three years. Given the table below:



Security product	Hardware price	Installation fee	Cost per message	Throughput	MTBF
DLP Vendor A	$50,000	$25,000	$1	100Mbps	10000 hours
DLP Vendor B	$38,000	$10,000	$2	50Mbps	8000 hours
DLP Vendor C	$45,000	$30,000	$1	70Mbps	7000 hours
DLP Vendor D	$40,000	$60,000	$0.50	100Mbps	7000 hours

Which of the following would be BEST for the CISO to include in this year’s budget?

A. A budget line for DLP Vendor A
B. A budget line for DLP Vendor B
C. A budget line for DLP Vendor C
D. A budget line for DLP Vendor D
E. A budget line for paying future fines

Correct Answer: E

Section: (none)
Explanation

Explanation/Reference:

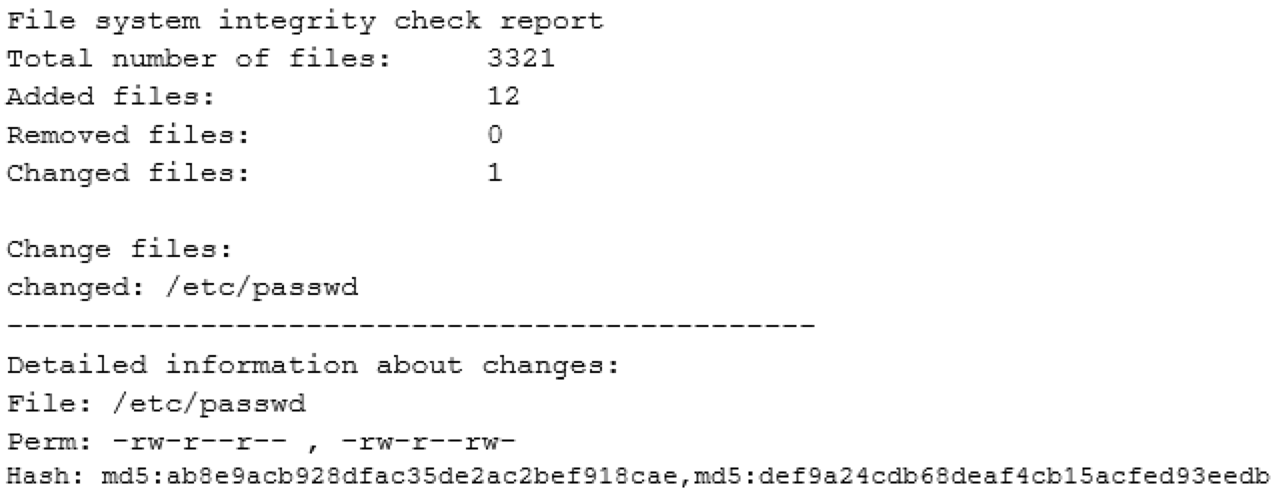
QUESTION 130
The Chief Information Security Officer (CISO) suspects that a database administrator has been tampering with financial data to the administrator’s advantage. Which of the following would allow a third-party consultant to conduct an on-site review of the administrator’s activity?

A. Separation of duties
B. Job rotation
C. Continuous monitoring
D. Mandatory vacation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
While investigating suspicious activity on a server, a security administrator runs the following report:



```
File system integrity check report
Total number of files:      3321
Added files:                12
Removed files:              0
Changed files:              1

Change files:
changed: /etc/passwd
----------------------------------------------
Detailed information about changes:
File: /etc/passwd
Perm: -rw-r--r-- , -rw-r--rw-
Hash: md5:ab8e9acb928dfac35de2ac2bef918cae,md5:def9a24cdb68deaf4cb15acfed93eedb
```

In addition, the administrator notices changes to the /etc/shadow file that were not listed in the report. Which of the following BEST describe this scenario? (Choose two.)

A. An attacker compromised the server and may have used a collision hash in the MD5 algorithm to hide the changes to the /etc/shadow file
B. An attacker compromised the server and may have also compromised the file integrity database to hide the changes to the /etc/shadow file
C. An attacker compromised the server and may have installed a rootkit to always generate valid MD5 hashes to hide the changes to the /etc/shadow file
D. An attacker compromised the server and may have used MD5 collision hashes to generate valid passwords, allowing further access to administrator accounts on the server
E. An attacker compromised the server and may have used SELinux mandatory access controls to hide the changes to the /etc/shadow file

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization’s incident response capabilities. Which of the following activities has the incident team lead executed?

A. Lessons learned review

B. Root cause analysis
C. Incident audit
D. Corrective action exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Following a recent network intrusion, a company wants to determine the current security awareness of all of its employees. Which of the following is the BEST way to test awareness?

A. Conduct a series of security training events with comprehensive tests at the end
B. Hire an external company to provide an independent audit of the network security posture
C. Review the social media of all employees to see how much proprietary information is shared
D. Send an email from a corporate account, requesting users to log onto a website with their enterprise account

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
A regional business is expecting a severe winter storm next week. The IT staff has been reviewing corporate policies on how to handle various situations and found some are missing or incomplete. After reporting this gap in documentation to the information security manager, a document is immediately drafted to move various personnel to other locations to avoid downtime in operations. This is an example of:

A. a disaster recovery plan
B. an incident response plan
C. a business continuity plan
D. a risk avoidance plan

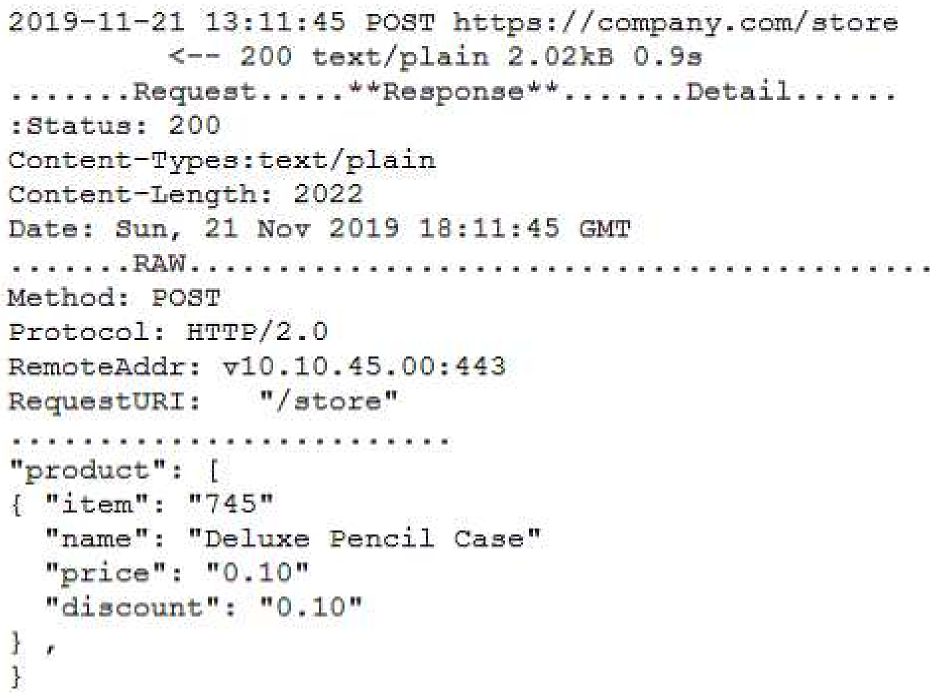
Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

A security engineer successfully exploits an application during a penetration test. As proof of the exploit, the security engineer takes screenshots of how data was compromised in the application. Given the information below from the screenshot.



```
2019-11-21 13:11:45 POST https://company.com/store
         <-- 200 text/plain 2.02kB 0.9s
.......Request.....**Response**.......Detail......
:Status: 200
Content-Types:text/plain
Content-Length: 2022
Date: Sun, 21 Nov 2019 18:11:45 GMT
.......RAW.........................................
Method: POST
Protocol: HTTP/2.0
RemoteAddr: v10.10.45.00:443
RequestURI:   "/store"
.........................
"product": [
{ "item": "745"
  "name": "Deluxe Pencil Case"
  "price": "0.10"
  "discount": "0.10"
} ,
}
```

Which of the following tools was MOST likely used to exploit the application?

A. The engineer captured the data with a protocol analyzer, and then utilized Python to edit the data

B. The engineer queried the server and edited the data using an HTTP proxy interceptor

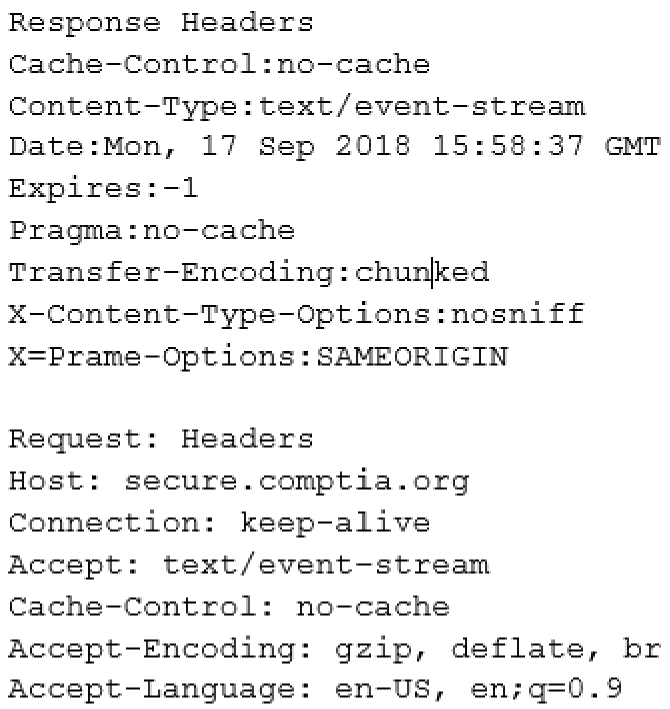
C. The engineer used a cross-site script sent via curl to edit the data

D. The engineer captured the HTTP headers, and then replaced the JSON data with a banner-grabbing tool

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
A security engineer is analyzing an application during a security assessment to ensure it is configured to protect against common threats. Given the output below:



```
Response Headers
Cache-Control:no-cache
Content-Type:text/event-stream
Date:Mon, 17 Sep 2018 15:58:37 GMT
Expires:-1
Pragma:no-cache
Transfer-Encoding:chunked
X-Content-Type-Options:nosniff
X=Prame-Options:SAMEORIGIN

Request: Headers
Host: secure.comptia.org
Connection: keep-alive
Accept: text/event-stream
Cache-Control: no-cache
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US, en;q=0.9
```

Which of the following tools did the security engineer MOST likely use to generate this output?

A. Application fingerprinter
B. Fuzzer
C. HTTP interceptor
D. Vulnerability scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
The Chief Financial Officer (CFO) of a major hospital system has received a ransom letter that demands a large sum of cryptocurrency be transferred to an anonymous account. If the transfer does not take place within ten hours, the letter states that patient information will be released on the dark web. A partial listing of recent patients is included in the letter. This is the first indication that a breach took place. Which of the following steps should be done FIRST?

A. Review audit logs to determine the extent of the breach
B. Pay the hacker under the condition that all information is destroyed
C. Engage a counter-hacking team to retrieve the data
D. Notify the appropriate legal authorities and legal counsel

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A project manager is working with system owners to develop maintenance windows for system pathing and upgrades in a cloud-based PaaS environment. Management has indicated one maintenance windows will be authorized per month, but clients have stated they require quarterly maintenance windows to meet their obligations. Which of the following documents should the project manager review?

A. MOU
B. SOW
C. SRTM
D. SLA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139

A Chief Information Security Officer (CISO) implemented MFA for all accounts in parallel with the BYOD policy. After the implementation, employees report the increased authentication method is causing increased time to tasks. This applies both to accessing the email client on the workstation and the online collaboration portal. Which of the following should be the CISO implement to address the employees' concerns?

A. Create an exception for the company's IPs.
B. Implement always-on VPN.
C. Configure the use of employee PKI authentication for email.
D. Allow the use of SSO.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140

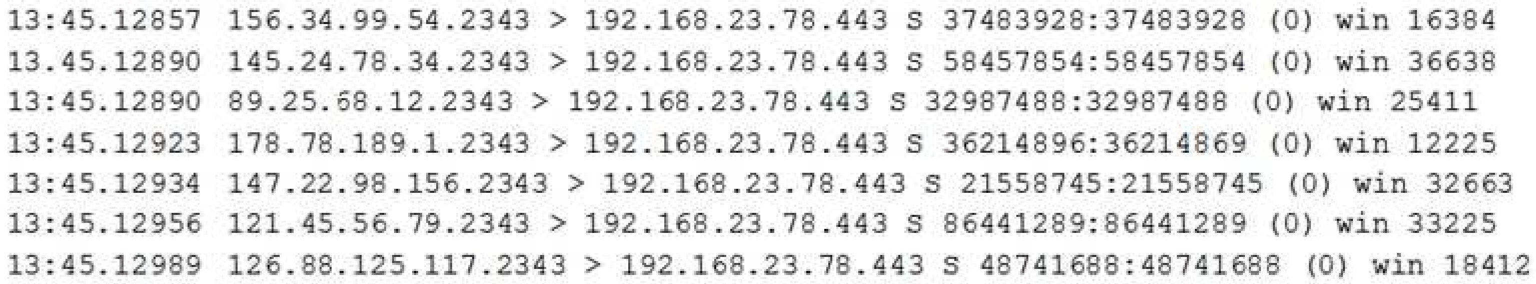
A Chief Information Security Officer (CISO) of a large financial institution undergoing an IT transformation program wants to embed security across the business rapidly and across as many layers of the business as possible to achieve quick wins and reduce risk to the organization. Which of the following business areas should the CISO target FIRST to best meet the objective?

A. Programmers and developers should be targeted to ensure secure coding practices, including automated code reviews with remediation processes, are implemented immediately.
B. Human resources should be targeted to ensure all new employees undertake security awareness and compliance training to reduce the impact of phishing and ransomware attacks.
C. The project management office should be targeted to ensure security is managed and included at all levels of the project management cycle for new and in-flight projects.
D. Risk assurance teams should be targeted to help identify key business unit security risks that can be aggregated across the organization to produce a risk posture dashboard for executive management.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
A university's help desk is receiving reports that Internet access on campus is not functioning. The network administrator looks at the management tools and sees the 1Gbps Internet is completely saturated with ingress traffic. The administrator sees the following output on the Internet router:



```
13:45.12857 156.34.99.54.2343 > 192.168.23.78.443 S 37483928:37483928 (0) win 16384
13.45.12890 145.24.78.34.2343 > 192.168.23.78.443 S 58457854:58457854 (0) win 36638
13:45.12890 89.25.68.12.2343 > 192.168.23.78.443 S 32987488:32987488 (0) win 25411
13:45.12923 178.78.189.1.2343 > 192.168.23.78.443 S 36214896:36214869 (0) win 12225
13:45.12934 147.22.98.156.2343 > 192.168.23.78.443 S 21558745:21558745 (0) win 32663
13:45.12956 121.45.56.79.2343 > 192.168.23.78.443 S 86441289:86441289 (0) win 33225
13:45.12989 126.88.125.117.2343 > 192.168.23.78.443 S 48741688:48741688 (0) win 18412
```

The administrator calls the university's ISP for assistance, but it takes more than four hours to speak to a network engineer who can resolve the problem. Based on the information above, which of the following should the ISP engineer do to resolve the issue?

A. The ISP engineer should null route traffic to the web server immediately to restore Internet connectivity. The university should implement a remotely triggered black hole with the ISP to resolve this more quickly in the future.
B. A university web server is under increased load during enrollment. The ISP engineer should immediately increase bandwidth to 2Gbps to restore Internet connectivity. In the future, the university should pay for more bandwidth to handle spikes in web server traffic.
C. The ISP engineer should immediately begin blocking IP addresses that are attacking the web server to restore Internet connectivity. In the future, the university should install a WAF to prevent this attack from happening again.
D. The ISP engineer should begin refusing network connections to the web server immediately to restore Internet connectivity on campus. The university should purchase an IPS device to stop DDoS attacks in the future.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A Chief Information Security Officer (CISO) recently changed jobs into a new industry. The CISO's first task is to write a new, relevant risk assessment for the organization. Which of the following help to the CISO find relevant risks to the organization? (Choose two.)

A. Perform a penetration test.

B. Conduct a regulatory audit.
C. Hire a third-party consultant.
D. Define the threat model.
E. Review the existing BIA.
F. Perform an attack path analysis.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference: