CompTIA

Exam Questions CAS-002

CompTIA Advanced Security Practitioner (CASP)

NEW QUESTION 1
- (Topic 1)
Ann, a software developer, wants to publish her newly developed software to an online store. Ann wants to ensure that the software will not be modified by a third party or end users before being installed on mobile devices. Which of the following should Ann implement to stop modified copies of her software from running on mobile devices?

A. Single sign-on
B. Identity propagation
C. Remote attestation
D. Secure code review

Answer: C

NEW QUESTION 2
- (Topic 1)
A security manager has received the following email from the Chief Financial Officer (CFO):
“While I am concerned about the security of the proprietary financial data in our ERP application, we have had a lot of turnover in the accounting group and I am having a difficult time meeting our monthly performance targets. As things currently stand, we do not allow employees to work from home but this is something I am willing to allow so we can get back on track. What should we do first to securely enable this capability for my group?”
Based on the information provided, which of the following would be the MOST appropriate response to the CFO?

A. Remote access to the ERP tool introduces additional security vulnerabilities and should not be allowed.
B. Allow VNC access to corporate desktops from personal computers for the users working from home.
C. Allow terminal services access from personal computers after the CFO provides a list of the users working from home.
D. Work with the executive management team to revise policies before allowing any remote access.

Answer: D

NEW QUESTION 3
- (Topic 1)
The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social media. Which of the following decisions is BEST for the CEO to make?

A. Social media is an effective solution because it is easily adaptable to new situations.
B. Social media is an ineffective solution because the policy may not align with the business.
C. Social media is an effective solution because it implements SSL encryption.
D. Social media is an ineffective solution because it is not primarily intended for business applications.

Answer: B

NEW QUESTION 4
- (Topic 1)
A web services company is planning a one-time high-profile event to be hosted on the corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?

A. Ensure web services hosting the event use TCP cookies and deny_hosts.
B. Configure an intrusion prevention system that blocks IPs after detecting too many incomplete sessions.
C. Contract and configure scrubbing services with third-party DDoS mitigation providers.
D. Purchase additional bandwidth from the company’s Internet service provider.

Answer: C

NEW QUESTION 5
- (Topic 1)
Company XYZ provides hosting services for hundreds of companies across multiple industries including healthcare, education, and manufacturing. The security architect for company XYZ is reviewing a vendor proposal to reduce company XYZ’s hardware costs by combining multiple physical hosts through the use of virtualization technologies. The security architect notes concerns about data separation, confidentiality, regulatory
requirements concerning PII, and administrative complexity on the proposal. Which of the following BEST describes the core concerns of the security architect?

A. Most of company XYZ’s customers are willing to accept the risks of unauthorized disclosure and access to information by outside users.
B. The availability requirements in SLAs with each hosted customer would have to be re- written to account for the transfer of virtual machines between physical platforms for regular maintenance.
C. Company XYZ could be liable for disclosure of sensitive data from one hosted customer when accessed by a malicious user who has gained access to the virtual machine of another hosted customer.
D. Not all of company XYZ’s customers require the same level of security and the administrative complexity of maintaining multiple security postures on a single hypervisor negates hardware cost savings.

Answer: C

NEW QUESTION 6
- (Topic 1)
An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO).

A. LDAP/S
B. SAML
C. NTLM
D. OAUTH
E. Kerberos

Answer: BE

NEW QUESTION 7
- (Topic 1)
A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

A. During the Identification Phase
B. During the Lessons Learned phase
C. During the Containment Phase
D. During the Preparation Phase

Answer: B

NEW QUESTION 8
- (Topic 1)
An intruder was recently discovered inside the data center, a highly sensitive area. To gain access, the intruder circumvented numerous layers of physical and electronic security measures. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again. Which of the following departments are the
MOST heavily invested in rectifying the problem? (Select THREE).

A. Facilities management
B. Human resources
C. Research and development
D. Programming
E. Data center operations
F. Marketing
G. Information technology

Answer: AEG

NEW QUESTION 9
- (Topic 1)
A penetration tester is assessing a mobile banking application. Man-in-the-middle attempts via a HTTP intercepting proxy are failing with SSL errors. Which of the following controls has likely been implemented by the developers?

A. SSL certificate revocation
B. SSL certificate pinning
C. Mobile device root-kit detection
D. Extended Validation certificates

Answer: B

NEW QUESTION 10
- (Topic 1)
A security company is developing a new cloud-based log analytics platform. Its purpose is to allow:
Which of the following are the BEST security considerations to protect data from one customer being disclosed to other customers? (Select THREE).

A. Secure storage and transmission of API keys
B. Secure protocols for transmission of log files and search results
C. At least two years retention of log files in case of e-discovery requests
D. Multi-tenancy with RBAC support
E. Sanitizing filters to prevent upload of sensitive log file contents
F. Encryption of logical volumes on which the customers' log files reside

Answer: :ABD

NEW QUESTION 10
- (Topic 1)
A security administrator is tasked with implementing two-factor authentication for the company VPN. The VPN is currently configured to authenticate VPN users against a backend RADIUS server. New company policies require a second factor of authentication, and the Information Security Officer has selected PKI as the second factor. Which of the following should the security administrator configure and implement on the VPN concentrator to implement the second factor and ensure that no error messages are displayed to the user during the VPN connection? (Select TWO).

A. The user’s certificate private key must be installed on the VPN concentrator.
B. The CA’s certificate private key must be installed on the VPN concentrator.
C. The user certificate private key must be signed by the CA.
D. The VPN concentrator’s certificate private key must be signed by the CA and installed on the VPN concentrator.
E. The VPN concentrator’s certificate private key must be installed on the VPN concentrator.
F. The CA’s certificate public key must be installed on the VPN concentrator.

Answer: EF

NEW QUESTION 13
- (Topic 1)
Company XYZ provides cable television service to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to keep the subsidiaries separate from the parent company. However all three companies must share customer data for the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies. Which of the following solutions is BEST suited for this scenario?

A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.
B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.
C. The companies should federate, with the parent becoming the IdP, and the subsidiaries
D. becoming an SP.
E. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Answer: C

NEW QUESTION 17
- (Topic 1)
The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

A. PING
B. NESSUS
C. NSLOOKUP
D. NMAP

Answer: D

NEW QUESTION 19
- (Topic 1)
A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

A. Client side input validation
B. Stored procedure
C. Encrypting credit card details
D. Regular expression matching

Answer: D

NEW QUESTION 21
- (Topic 1)
The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).

A. Retrieve source system image from backup and run file comparison analysis on the two images.
B. Parse all images to determine if extra data is hidden using steganography.
C. Calculate a new hash and compare it with the previously captured image hash.
D. Ask desktop support if any changes to the images were made.
E. Check key system files to see if date/time stamp is in the past six months.

Answer: AC

NEW QUESTION 23
- (Topic 1)
A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of
$100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent
B. 5.5 percent
C. 45 percent
D. 82 percent

Answer: D

NEW QUESTION 26
- (Topic 1)
A new internal network segmentation solution will be implemented into the enterprise that consists of 200 internal firewalls. As part of running a pilot exercise, it was determined that it takes three changes to deploy a new application onto the network before it is operational. Security now has a significant effect on overall availability. Which of the following would be the FIRST process to perform as a result of these findings?

A. Lower the SLA to a more tolerable level and perform a risk assessment to see if the solution could be met by another solutio
B. Reuse the firewall infrastructure on other projects.

C. Perform a cost benefit analysis and implement the solution as it stands as long as the risks are understood by the business owners around the availability issue
D. Decrease the current SLA expectations to match the new solution.
E. Engage internal auditors to perform a review of the project to determine why and how the project did not meet the security requirement
F. As part of the review ask them to review the control effectiveness.
G. Review to determine if control effectiveness is in line with the complexity of the solutio
H. Determine if the requirements can be met with a simpler solution.

Answer: D

NEW QUESTION 27
- (Topic 1)
The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

A. The corporate network is the only network that is audited by regulators and customers.
B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.
C. Home networks are unknown to attackers and less likely to be targeted directly.
D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Answer: B

NEW QUESTION 31
- (Topic 1)
A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

A. Agile
B. SDL
C. Waterfall
D. Joint application development

Answer: A

NEW QUESTION 35
- (Topic 1)
The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

A. Block traffic from the ISP's networks destined for blacklisted IPs.
B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.
C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.
D. Notify customers when services they run are involved in an attack.
E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.

Answer: DE

NEW QUESTION 38
- (Topic 1)
A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
B. A DLP gateway should be installed at the company border.
C. Strong authentication should be implemented via external biometric devices.
D. Full-tunnel VPN should be required for all network communication.
E. Full-drive file hashing should be implemented with hashes stored on separate storage.
F. Split-tunnel VPN should be enforced when transferring sensitive data.

Answer: BD

NEW QUESTION 42
- (Topic 1)
An industry organization has implemented a system to allow trusted authentication between all of its partners. The system consists of a web of trusted RADIUS servers communicating over the Internet. An attacker was able to set up a malicious server and conduct a successful man-in-the-middle attack. Which of the following controls should be implemented to mitigate the attack in the future?

A. Use PAP for secondary authentication on each RADIUS server
B. Disable unused EAP methods on each RADIUS server
C. Enforce TLS connections between RADIUS servers
D. Use a shared secret for each pair of RADIUS servers

Answer: C

NEW QUESTION 47
- (Topic 1)
A security administrator is shown the following log excerpt from a Unix system:
2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port 37914 ssh2
2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port 37915 ssh2
2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port 37916 ssh2
2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port 37918 ssh2
2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port 37920 ssh2
2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port 37924 ssh2
Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

A. An authorized administrator has logged into the root account remotely.
B. The administrator should disable remote root logins.
C. Isolate the system immediately and begin forensic analysis on the host.
D. A remote attacker has compromised the root account using a buffer overflow in sshd.
E. A remote attacker has guessed the root password using a dictionary attack.
F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
G. A remote attacker has compromised the private key of the root account.
H. Change the root password immediately to a password not found in a dictionary.

Answer: CE

NEW QUESTION 51
- (Topic 1)
After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

A. Least privilege
B. Job rotation
C. Mandatory vacation
D. Separation of duties

Answer: B

NEW QUESTION 53
- (Topic 1)
An external penetration tester compromised one of the client organization’s authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization’s other systems, without impacting the integrity of any of the systems?

A. Use the pass the hash technique
B. Use rainbow tables to crack the passwords
C. Use the existing access to change the password
D. Use social engineering to obtain the actual password

Answer: A

NEW QUESTION 55
- (Topic 1)
The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?

A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
B. Improper handling of client data, interoperability agreement issues and regulatory issues
C. Cultural differences, increased cost of doing business and divestiture issues
D. Improper handling of customer data, loss of intellectual property and reputation damage

Answer: D

NEW QUESTION 59
- (Topic 1)
The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

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

Answer: C

NEW QUESTION 61
- (Topic 1)
The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:
11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400
11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400
Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.
B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.
C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks.
D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

Answer: :A

NEW QUESTION 63
- (Topic 1)
A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs
B. Interview employees and managers to discover the industry hot topics and trends
C. Attend meetings with staff, internal training, and become certified in software management
D. Attend conferences, webinars, and training to remain current with the industry and job requirements

Answer: D

NEW QUESTION 67
- (Topic 1)
An attacker attempts to create a DoS event against the VoIP system of a company. The attacker uses a tool to flood the network with a large number of SIP INVITE traffic. Which of the following would be LEAST likely to thwart such an attack?

A. Install IDS/IPS systems on the network
B. Force all SIP communication to be encrypted
C. Create separate VLANs for voice and data traffic
D. Implement QoS parameters on the switches

Answer: D

NEW QUESTION 71
- (Topic 1)
The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:
90.76.165.40 – - [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724
90.76.165.40 – - [08/Mar/2014:10:54:05] "GET ../../../root/.bash_history HTTP/1.1" 200
5724
90.76.165.40 – - [08/Mar/2014:10:54:04] "GET index.php?user=<script>Create</script> HTTP/1.1" 200 5724
The security administrator also inspects the following file system locations on the database server using the command 'ls -al /root'
drwxrwxrwx 11 root root 4096 Sep 28 22:45 .
drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..
-rws------ 25 root root 4096 Mar 8 09:30 .bash_history
-rw------- 25 root root 4096 Mar 8 09:30 .bash_history
-rw------- 25 root root 4096 Mar 8 09:30 .profile
-rw------- 25 root root 4096 Mar 8 09:30 .ssh
Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

A. Privilege escalation
B. Brute force attack
C. SQL injection
D. Cross-site scripting
E. Using input validation, ensure the following characters are sanitized: <>
F. Update crontab with: find / \(-perm -4000 \) –type f –print0 | xargs -0 ls –l | email.sh
G. Implement the following PHP directive: $clean_user_input = addslashes($user_input)
H. Set an account lockout policy

Answer: AF

NEW QUESTION 75
- (Topic 1)
The administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Which of the following issues may potentially occur?

A. The data may not be in a usable format.
B. The new storage array is not FCoE based.
C. The data may need a file system check.
D. The new storage array also only has a single controller.

Answer: A

NEW QUESTION 77
- (Topic 1)
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation
B. Security test and evaluation
C. Risk assessment
D. Ongoing authorization

Answer: D

NEW QUESTION 78
- (Topic 1)
A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.
B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.
C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.
D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Answer: A

NEW QUESTION 80
- (Topic 1)
A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO's requirement?

A. GRC
B. IPS
C. CMDB
D. Syslog-ng
E. IDS

Answer: A

NEW QUESTION 85
- (Topic 1)
During a recent audit of servers, a company discovered that a network administrator, who required remote access, had deployed an unauthorized remote access application that communicated over common ports already allowed through the firewall. A network scan showed that this remote access application had already been installed on one third of the servers in the company. Which of the following is the MOST appropriate action that the company should take to provide a more appropriate solution?

A. Implement an IPS to block the application on the network
B. Implement the remote application out to the rest of the servers
C. Implement SSL VPN with SAML standards for federation
D. Implement an ACL on the firewall with NAT for remote access

Answer: C

NEW QUESTION 86
- (Topic 1)
A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

A. RAS
B. Vulnerability scanner
C. HTTP intercept

D. HIDS
E. Port scanner
F. Protocol analyzer

Answer: DF

NEW QUESTION 90
- (Topic 1)
An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

A. Guest users could present a risk to the integrity of the company's information
B. Authenticated users could sponsor guest access that was previously approved by management
C. Unauthenticated users could present a risk to the confidentiality of the company's information
D. Meeting owners could sponsor guest access if they have passed a background check

Answer: C

NEW QUESTION 95
- (Topic 1)
A forensic analyst works for an e-discovery firm where several gigabytes of data are processed daily. While the business is lucrative, they do not have the resources or the scalability to adequately serve their clients. Since it is an e-discovery firm where chain of custody is important, which of the following scenarios should they consider?

A. Offload some data processing to a public cloud
B. Aligning their client intake with the resources available
C. Using a community cloud with adequate controls
D. Outsourcing the service to a third party cloud provider

Answer: C

NEW QUESTION 96
- (Topic 1)
A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on exploits and information security news?

A. Update company policies and procedures
B. Subscribe to security mailing lists
C. Implement security awareness training
D. Ensure that the organization vulnerability management plan is up-to-date

Answer: B

NEW QUESTION 100
- (Topic 1)
Due to a new regulatory requirement, ABC Company must now encrypt all WAN transmissions. When speaking with the network administrator, the security administrator learns that the existing routers have the minimum processing power to do the required level of encryption. Which of the following solutions minimizes the performance impact on the router?

A. Deploy inline network encryption devices
B. Install an SSL acceleration appliance
C. Require all core business applications to use encryption
D. Add an encryption module to the router and configure IPSec

Answer: A

NEW QUESTION 104
- (Topic 1)
The helpdesk manager wants to find a solution that will enable the helpdesk staff to better serve company employees who call with computer-related problems. The helpdesk staff is currently unable to perform effective troubleshooting and relies on callers to describe their technology problems. Given that the helpdesk staff is located within the company headquarters and 90% of the callers are telecommuters, which of the following tools should the helpdesk manager use to make the staff more effective at troubleshooting while at the same time reducing company costs? (Select TWO).

A. Web cameras
B. Email
C. Instant messaging
D. BYOD
E. Desktop sharing
F. Presence

Answer: CE

NEW QUESTION 106
- (Topic 1)
Joe, the Chief Executive Officer (CEO), was an Information security professor and a Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which

of the following methodologies should be adopted?

A. The company should develop an in-house solution and keep the algorithm a secret.
B. The company should use the CEO's encryption scheme.
C. The company should use a mixture of both systems to meet minimum standards.
D. The company should use the method recommended by other respected information security organizations.

Answer: D

NEW QUESTION 111
- (Topic 1)
The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.
B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
C. Publish a policy that addresses the security requirements for working remotely with company equipment.
D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Answer: C

NEW QUESTION 113
- (Topic 1)
A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

A. Code review
B. Penetration testing
C. Grey box testing
D. Code signing
E. White box testing

Answer: AE

NEW QUESTION 118
- (Topic 1)
Due to compliance regulations, a company requires a yearly penetration test. The Chief Information Security Officer (CISO) has asked that it be done under a black box methodology.
Which of the following would be the advantage of conducting this kind of penetration test?

A. The risk of unplanned server outages is reduced.
B. Using documentation provided to them, the pen-test organization can quickly determine areas to focus on.
C. The results will show an in-depth view of the network and should help pin-point areas of internal weakness.
D. The results should reflect what attackers may be able to learn about the company.

Answer: D

NEW QUESTION 123
- (Topic 1)
The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.
D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Answer: A

NEW QUESTION 126
- (Topic 1)
A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this
policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

A. Establish a risk matrix
B. Inherit the risk for six months
C. Provide a business justification to avoid the risk
D. Provide a business justification for a risk exception

Answer: D

NEW QUESTION 128

- (Topic 1)
There have been some failures of the company's internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month's performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?

A. 92.24 percent
B. 98.06 percent
C. 98.34 percent
D. 99.72 percent

Answer: C

NEW QUESTION 132
- (Topic 1)
A security administrator wants to deploy a dedicated storage solution which is inexpensive, can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

A. SAN
B. NAS
C. Virtual SAN
D. Virtual storage

Answer: B

NEW QUESTION 135
- (Topic 1)
Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform?

A. Aggressive patch management on the host and guest OSs.
B. Host based IDS sensors on all guest OSs.
C. Different antivirus solutions between the host and guest OSs.
D. Unique Network Interface Card (NIC) assignment per guest OS.

Answer: A

NEW QUESTION 137
- (Topic 1)
At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

A. Add guests with more memory to increase capacity of the infrastructure.
B. A backup is running on the thin clients at 9am every morning.
C. Install more memory in the thin clients to handle the increased load while booting.
D. Booting all the lab desktops at the same time is creating excessive I/O.
E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.
F. Install faster SSD drives in the storage system used in the infrastructure.
G. The lab desktops are saturating the network while booting.
H. The lab desktops are using more memory than is available to the host systems.

Answer: DF

NEW QUESTION 139
- (Topic 1)
A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self service functionality. The application has been written by developers over the last six months and the project is currently in the test phase.
Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over the solution? (Select TWO).

A. Perform unit testing of the binary code
B. Perform code review over a sampling of the front end source code
C. Perform black box penetration testing over the solution
D. Perform grey box penetration testing over the solution
E. Perform static code review over the front end source code

Answer: DE

NEW QUESTION 144
- (Topic 1)
A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

A. Insecure direct object references, CSRF, Smurf
B. Privilege escalation, Application DoS, Buffer overflow
C. SQL injection, Resource exhaustion, Privilege escalation
D. CSRF, Fault injection, Memory leaks

Answer: A

NEW QUESTION 145
- (Topic 1)
A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition
B. Encryption of the SSD at the file level
C. FDE of each logical volume on the SSD
D. FDE of the entire SSD as a single disk

Answer: A

NEW QUESTION 149
- (Topic 1)
Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the
penetration tester MOST likely to use while performing black box testing of the security of the company's purchased application? (Select TWO).

A. Code review
B. Sandbox
C. Local proxy
D. Fuzzer
E. Port scanner

Answer: CD

NEW QUESTION 153
- (Topic 1)
A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

A. Spiral model
B. Incremental model
C. Waterfall model
D. Agile model

Answer: C

NEW QUESTION 154
- (Topic 1)
A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and requires two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.
D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Answer: AD

NEW QUESTION 155
- (Topic 1)
A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

A. Agile
B. Waterfall
C. Scrum
D. Spiral

Answer: :B

NEW QUESTION 156
- (Topic 1)
Company A needs to export sensitive data from its financial system to company B's database, using company B's API in an automated manner. Company A's policy prohibits the use of any intermediary external systems to transfer or store its sensitive data, therefore the transfer must occur directly between company A's financial system and company B's destination server using the supplied API. Additionally, company A's legacy financial software does not support encryption, while company B's API supports encryption. Which of the following will provide end-to-end encryption for the data transfer while adhering to these requirements?

A. Company A must install an SSL tunneling software on the financial system.
B. Company A's security administrator should use an HTTPS capable browser to transfer the data.
C. Company A should use a dedicated MPLS circuit to transfer the sensitive data to company B.
D. Company A and B must create a site-to-site IPSec VPN on their respective firewalls.

Answer: A

NEW QUESTION 158
- (Topic 2)
A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.
To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

A. Residual Risk calculation
B. A cost/benefit analysis
C. Quantitative Risk Analysis
D. Qualitative Risk Analysis

Answer: C

NEW QUESTION 160
- (Topic 2)
The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

A. Capture process ID data and submit to anti-virus vendor for review.
B. Reboot the Linux servers, check running processes, and install needed patches.
C. Remove a single Linux server from production and place in quarantine.
D. Notify upper management of a security breach.
E. Conduct a bit level image, including RAM, of one or more of the Linux servers.

Answer: E

NEW QUESTION 165
- (Topic 2)
A new IT company has hired a security consultant to implement a remote access system, which will enable employees to telecommute from home using both company issued as well as personal computing devices, including mobile devices. The company wants a flexible system to provide confidentiality and integrity for data in transit to the company's internally developed application GUI. Company policy prohibits employees from having administrative rights to company issued devices. Which of the following remote access solutions has the lowest technical complexity?

A. RDP server
B. Client-based VPN
C. IPSec
D. Jump box
E. SSL VPN

Answer: A

NEW QUESTION 170
- (Topic 2)
Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:
POST /login.aspx HTTP/1.1 Host: comptia.org
Content-type: text/html txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true
Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

A. Remove all of the post data and change the request to /login.aspx from POST to GET
B. Attempt to brute force all usernames and passwords using a password cracker
C. Remove the txtPassword post data and change alreadyLoggedIn from false to true
D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

Answer: C

NEW QUESTION 172
- (Topic 2)
VPN users cannot access the active FTP server through the router but can access any
server in the data center.
Additional network information:
DMZ network – 192.168.5.0/24 (FTP server is 192.168.5.11) VPN network – 192.168.1.0/24
Datacenter – 192.168.2.0/24 User network - 192.168.3.0/24 HR network – 192.168.4.0/24\
Traffic shaper configuration: VLAN Bandwidth Limit (Mbps) VPN50
User175 HR250
Finance250 Guest0
Router ACL: ActionSourceDestination Permit192.168.1.0/24192.168.2.0/24 Permit192.168.1.0/24192.168.3.0/24 Permit192.168.1.0/24192.168.5.0/24
Permit192.168.2.0/24192.168.1.0/24 Permit192.168.3.0/24192.168.1.0/24 Permit192.168.5.1/32192.168.1.0/24 Deny192.168.4.0/24192.168.1.0/24
Deny192.168.1.0/24192.168.4.0/24

Denyanyany
Which of the following solutions would allow the users to access the active FTP server?

A. Add a permit statement to allow traffic from 192.168.5.0/24 to the VPN network
B. Add a permit statement to allow traffic to 192.168.5.1 from the VPN network
C. IPS is blocking traffic and needs to be reconfigured
D. Configure the traffic shaper to limit DMZ traffic
E. Increase bandwidth limit on the VPN network

Answer: A

NEW QUESTION 176
- (Topic 2)
A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

A. Subjective and based on an individual's experience.
B. Requires a high degree of upfront work to gather environment details.
C. Difficult to differentiate between high, medium, and low risks.
D. Allows for cost and benefit analysis.
E. Calculations can be extremely complex to manage.

Answer: A

NEW QUESTION 177
- (Topic 2)
ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

A. Establish a list of users that must work with each regulation
B. Establish a list of devices that must meet each regulation
C. Centralize management of all devices on the network
D. Compartmentalize the network
E. Establish a company framework
F. Apply technical controls to meet compliance with the regulation

Answer: BDF

NEW QUESTION 180
- (Topic 2)
Customers have recently reported incomplete purchase history and other anomalies while accessing their account history on the web server farm. Upon investigation, it has been determined that there are version mismatches of key e-commerce applications on the production web servers. The development team has direct access to the production servers and is most likely the cause of the different release versions. Which of the following process level solutions would address this problem?

A. Implement change control practices at the organization level.
B. Adjust the firewall ACL to prohibit development from directly accessing the production server farm.
C. Update the vulnerability management plan to address data discrepancy issues.
D. Change development methodology from strict waterfall to agile.

Answer: A

NEW QUESTION 183
- (Topic 2)
An employee is performing a review of the organization’s security functions and noticed that there is some cross over responsibility between the IT security team and the financial fraud team. Which of the following security documents should be used to clarify the roles and responsibilities between the teams?

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

Answer: C

NEW QUESTION 188
- (Topic 2)
A bank has decided to outsource some existing IT functions and systems to a third party service provider. The third party service provider will manage the outsourced systems on their own premises and will continue to directly interface with the bank’s other systems through dedicated encrypted links. Which of the following is critical to ensure the successful management of system security concerns between the two organizations?

A. ISA
B. BIA
C. MOU
D. SOA
E. BPA

Answer: A

NEW QUESTION 190
- (Topic 2)
Joe is a security architect who is tasked with choosing a new NIPS platform that has the ability to perform SSL inspection, analyze up to 10Gbps of traffic, can be centrally managed and only reveals inspected application payload data to specified internal security employees. Which of the following steps should Joe take to reach the desired outcome?

A. Research new technology vendors to look for potential product
B. Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product meets all mandatory requirement
C. Test the product and make a product recommendation.
D. Evaluate relevant RFC and ISO standards to choose an appropriate vendor produc
E. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased.
F. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.
G. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provide
H. Give access to internal security employees so that they can inspect the application payload data.
I. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.

Answer: A

NEW QUESTION 194
- (Topic 2)
Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

A. Establish a cloud-based authentication service that supports SAML.
B. Implement a new Diameter authentication server with read-only attestation.
C. Install a read-only Active Directory server in the corporate DMZ for federation.
D. Allow external connections to the existing corporate RADIUS server.

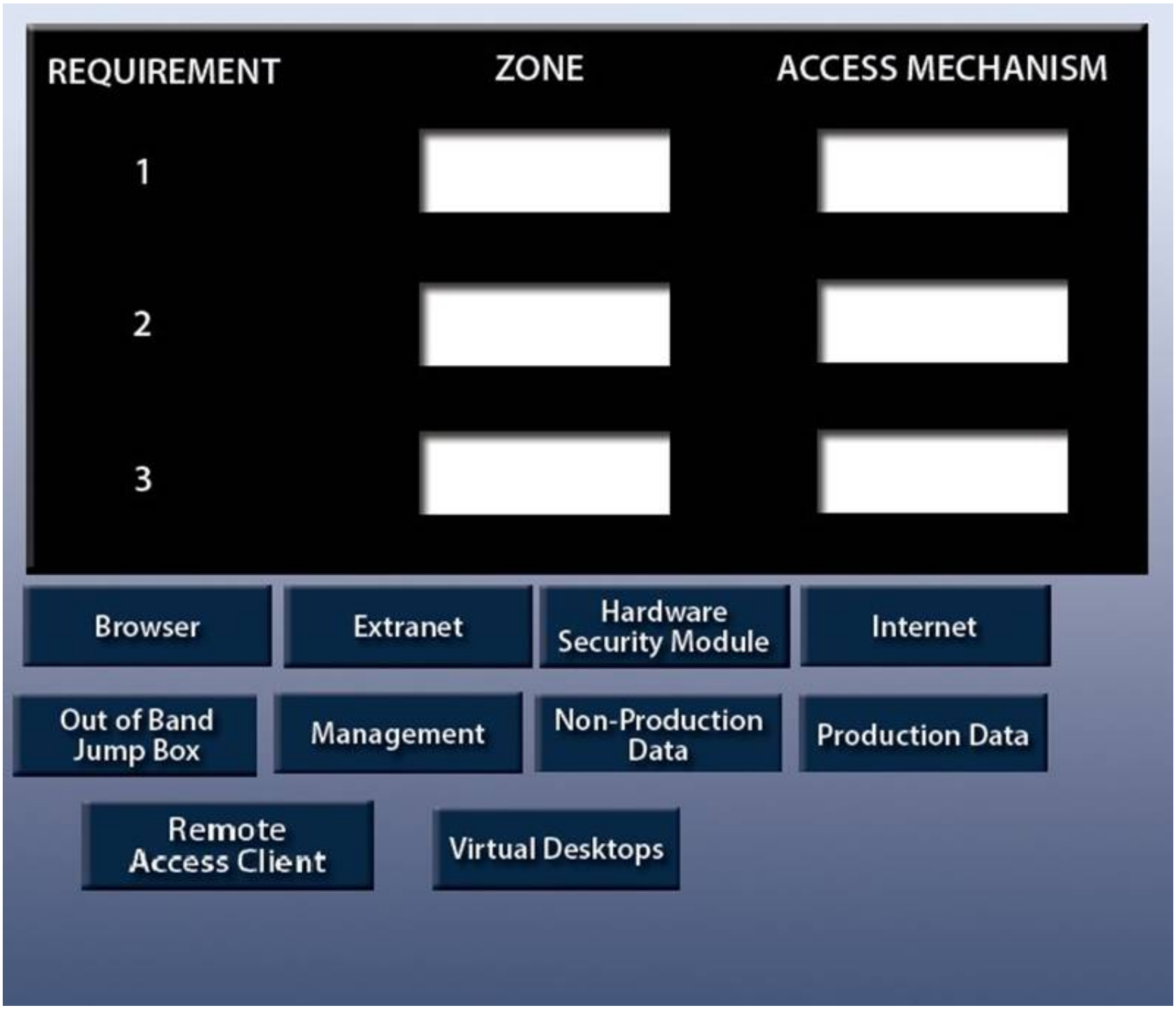
Answer: A

NEW QUESTION 199
- (Topic 2)
A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

A. Use AES in Electronic Codebook mode
B. Use RC4 in Cipher Block Chaining mode
C. Use RC4 with Fixed IV generation
D. Use AES with cipher text padding
E. Use RC4 with a nonce generated IV
F. Use AES in Counter mode

Answer: EF

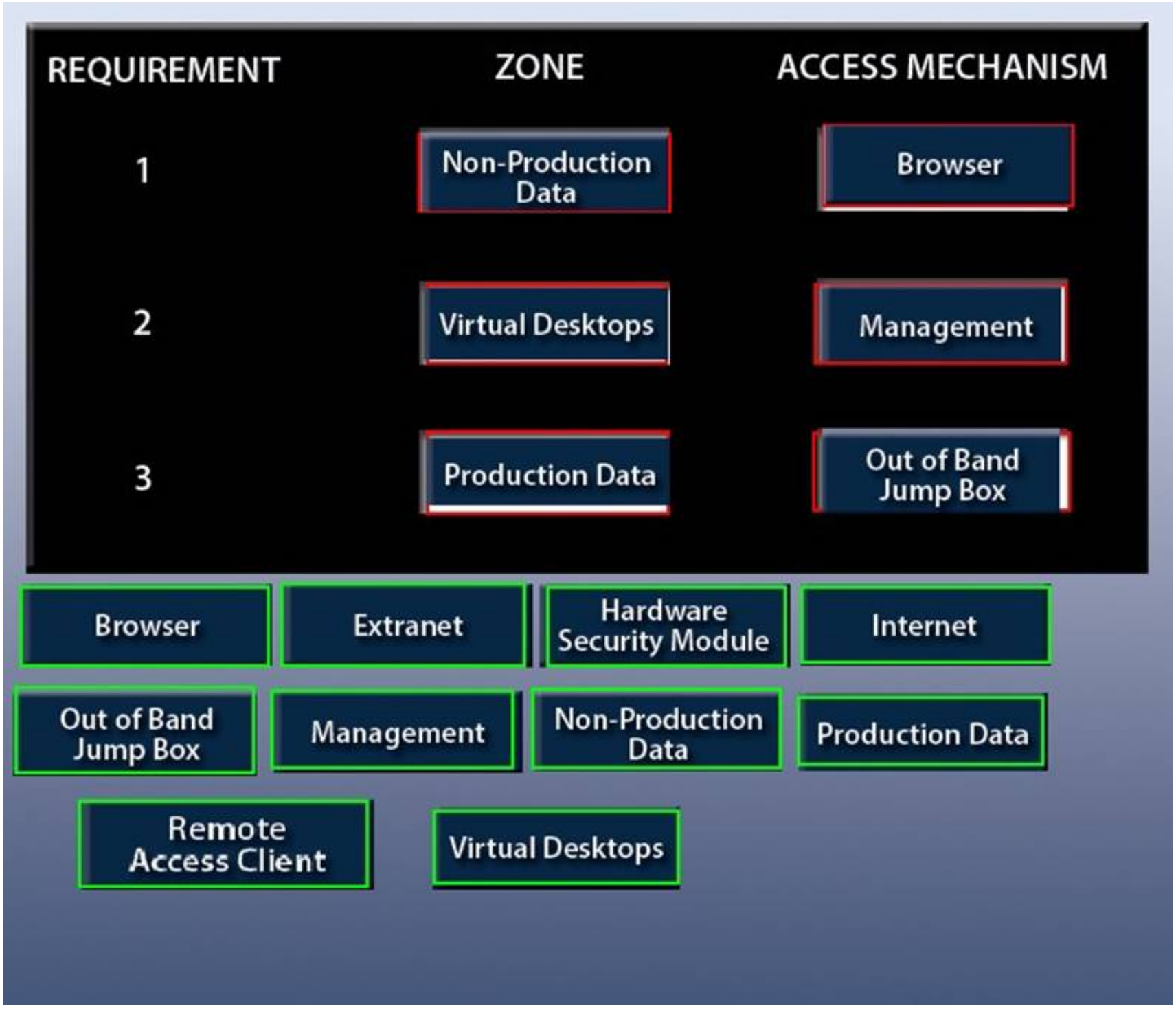
NEW QUESTION 202
DRAG DROP - (Topic 2)
A manufacturer is planning to build a segregated network. There are requirements to segregate development and test infrastructure from production and the need to support multiple entry points into the network depending on the service being accessed. There are also strict rules in place to only permit user access from within the same zone. Currently, the following access requirements have been identified:
1. Developers have the ability to perform technical validation of development applications.
2. End users have the ability to access internal web applications.
3. Third-party vendors have the ability to support applications.
In order to meet segregation and access requirements, drag and drop the appropriate network zone that the user would be accessing and the access mechanism to meet the above criteria. Options may be used once or not at all. All placeholders must be filled.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 206
- (Topic 2)
The IT director has charged the company helpdesk with sanitizing fixed and removable media. The helpdesk manager has written a new procedure to be followed by the helpdesk staff. This procedure includes the current standard to be used for data sanitization, as well as the location of physical degaussing tools. In which of the following cases should the helpdesk staff use the new procedure? (Select THREE).

A. During asset disposal
B. While reviewing the risk assessment
C. While deploying new assets
D. Before asset repurposing
E. After the media has been disposed of
F. During the data classification process
G. When installing new printers
H. When media fails or is unusable

Answer: ADH

NEW QUESTION 209
- (Topic 2)
An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates $10,000 in revenue a month. The new software product has an initial cost of $180,000 and a yearly maintenance of $2,000 after the first year. However, it will generate $15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

A. 1
B. 2
C. 3
D. 4

Answer: D

NEW QUESTION 212
- (Topic 2)
The telecommunications manager wants to improve the process for assigning company- owned mobile devices and ensuring data is properly removed when no longer needed. Additionally, the manager wants to onboard and offboard personally owned mobile devices that will be used in the BYOD initiative. Which of the following should be implemented to ensure these processes can be automated? (Select THREE).

A. SIM's PIN
B. Remote wiping
C. Chargeback system
D. MDM software
E. Presence software
F. Email profiles
G. Identity attestation
H. GPS tracking

Answer: BDG

NEW QUESTION 217
- (Topic 2)
After reviewing a company's NAS configuration and file system access logs, the auditor is advising the security administrator to implement additional security controls on the NFS export. The security administrator decides to remove the no_root_squash directive from the export and add the nosuid directive. Which of the following is true about the security controls implemented by the security administrator?

A. The newly implemented security controls are in place to ensure that NFS encryption can only be controlled by the root user.
B. Removing the no_root_squash directive grants the root user remote NFS read/write access to important files owned by root on the NAS.
C. Users with root access on remote NFS client computers can always use the SU command to modify other user's files on the NAS.
D. Adding the nosuid directive disables regular users from accessing files owned by the root user over NFS even after using the SU command.

Answer: C

NEW QUESTION 222
- (Topic 2)
ODBC access to a database on a network-connected host is required. The host does not have a security mechanism to authenticate the incoming ODBC connection, and the application requires that the connection have read/write permissions. In order to further secure the data, a nonstandard configuration would need to be implemented. The information in the database is not sensitive, but was not readily accessible prior to the implementation of the ODBC connection. Which of the following actions should be taken by the security analyst?

A. Accept the risk in order to keep the system within the company's standard security configuration.
B. Explain the risks to the data owner and aid in the decision to accept the risk versus choosing a nonstandard solution.
C. Secure the data despite the need to use a security control or solution that is not within company standards.
D. Do not allow the connection to be made to avoid unnecessary risk and avoid deviating from the standard security configuration.

Answer: B

NEW QUESTION 223
- (Topic 2)
A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations
B. Establish alerts at a certain threshold to notify the analyst of high activity
C. Provide a report showing the file transfer logs of the servers
D. Compare the current activity to the baseline of normal activity

Answer: D

NEW QUESTION 228
- (Topic 2)
A company provides on-demand cloud computing resources for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two- factor authentication for customer access to the administrative website. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data from customer A was found on a hidden directory within the VM of company B. Company B is not in the same industry as company A and the two are not competitors. Which of the following has MOST likely occurred?

A. Both VMs were left unsecured and an attacker was able to exploit network vulnerabilities to access each and move the data.
B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.
C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.
D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.

Answer: A

NEW QUESTION 230
- (Topic 2)
A security administrator was recently hired in a start-up company to represent the interest of security and to assist the network team in improving security in the company. The programmers are not on good terms with the security team and do not want to be distracted with security issues while they are working on a major project. Which of the following is the BEST time to make them address security issues in the project?

A. In the middle of the project
B. At the end of the project
C. At the inception of the project
D. At the time they request

Answer: C

NEW QUESTION 232
- (Topic 2)
A security tester is testing a website and performs the following manual query: https://www.comptia.com/cookies.jsp?products=5%20and%201=1
The following response is received in the payload: “ORA-000001: SQL command not properly ended”
Which of the following is the response an example of?

A. Fingerprinting
B. Cross-site scripting
C. SQL injection
D. Privilege escalation

Answer: A

NEW QUESTION 235
- (Topic 2)
After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

A. The binary files used by the application have been modified by malware.
B. The application is unable to perform remote attestation due to blocked ports.
C. The restored image backup was encrypted with the wrong key.
D. The hash key summary of hardware and installed software no longer match.

Answer: D

NEW QUESTION 240
- (Topic 2)
An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.
B. Implement a honey pot to capture traffic during the next attack.
C. Configure the servers for high availability to handle the additional bandwidth.
D. Log all traffic coming from the competitor's public IP addresses.

Answer: A

NEW QUESTION 241
- (Topic 2)
A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?

A. Use fuzzing techniques to examine application inputs
B. Run nmap to attach to application memory
C. Use a packet analyzer to inspect the strings
D. Initiate a core dump of the application
E. Use an HTTP interceptor to capture the text strings

Answer: D

NEW QUESTION 242
- (Topic 2)
Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ’s headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

A. Require each Company XYZ employee to use an IPSec connection to the required systems
B. Require Company XYZ employees to establish an encrypted VDI session to the required systems
C. Require Company ABC employees to use two-factor authentication on the required systems
D. Require a site-to-site VPN for intercompany communications

Answer: B

NEW QUESTION 246
- (Topic 2)
A security architect has been engaged during the implementation stage of the SDLC to review a new HR software installation for security gaps. With the project under a tight schedule to meet market commitments on project delivery, which of the following security activities should be prioritized by the security architect? (Select TWO).

A. Perform penetration testing over the HR solution to identify technical vulnerabilities
B. Perform a security risk assessment with recommended solutions to close off high-rated risks
C. Secure code review of the HR solution to identify security gaps that could be exploited
D. Perform access control testing to ensure that privileges have been configured correctly
E. Determine if the information security standards have been complied with by the project

Answer: BE

NEW QUESTION 250
- (Topic 2)
Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

A. Jailbroken mobile device
B. Reconnaissance tools
C. Network enumerator
D. HTTP interceptor
E. Vulnerability scanner
F. Password cracker

Answer: :DE

NEW QUESTION 252
CORRECT TEXT - (Topic 2)
Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several Internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:
User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet:192.168.3.0/24
Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down
Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.
Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.
Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.
Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

A.

Answer: Pleaselookintotheexplanationforthesolutiontothisquestion.

NEW QUESTION 256
- (Topic 2)
It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?

A. Update the blog page to HTTPS
B. Filter metacharacters
C. Install HIDS on the server
D. Patch the web application
E. Perform client side input validation

Answer: B

NEW QUESTION 261
- (Topic 2)
A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user's communicatio
B. Next, place a legal hold on the user's email account.
C. Perform an e-discover using the applicable search term
D. Next, back up the user's email for a future investigation.
E. Place a legal hold on the user's email accoun
F. Next, perform e-discovery searches to collect applicable emails.
G. Perform a back up of the user's email accoun
H. Next, export the applicable emails that match the search terms.

Answer: C

NEW QUESTION 262
- (Topic 2)
A facilities manager has observed varying electric use on the company's metered service lines. The facility management rarely interacts with the IT department unless new equipment is being delivered. However, the facility manager thinks that there is a correlation between spikes in electric use and IT department activity. Which of the following business processes and/or practices would provide better management of organizational resources with the IT department's needs? (Select TWO).

A. Deploying a radio frequency identification tagging asset management system
B. Designing a business resource monitoring system
C. Hiring a property custodian
D. Purchasing software asset management software
E. Facility management participation on a change control board
F. Rewriting the change board charter
G. Implementation of change management best practices

Answer: EG

NEW QUESTION 267
- (Topic 2)
A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

A. A review of the mitigations implemented from the most recent audit findings of the smaller company should be performed.
B. An ROI calculation should be performed to determine which company's application should be used.
C. A security assessment should be performed to establish the risks of integration or co- existence.
D. A regression test should be performed on the in-house software to determine security risks associated with the software.

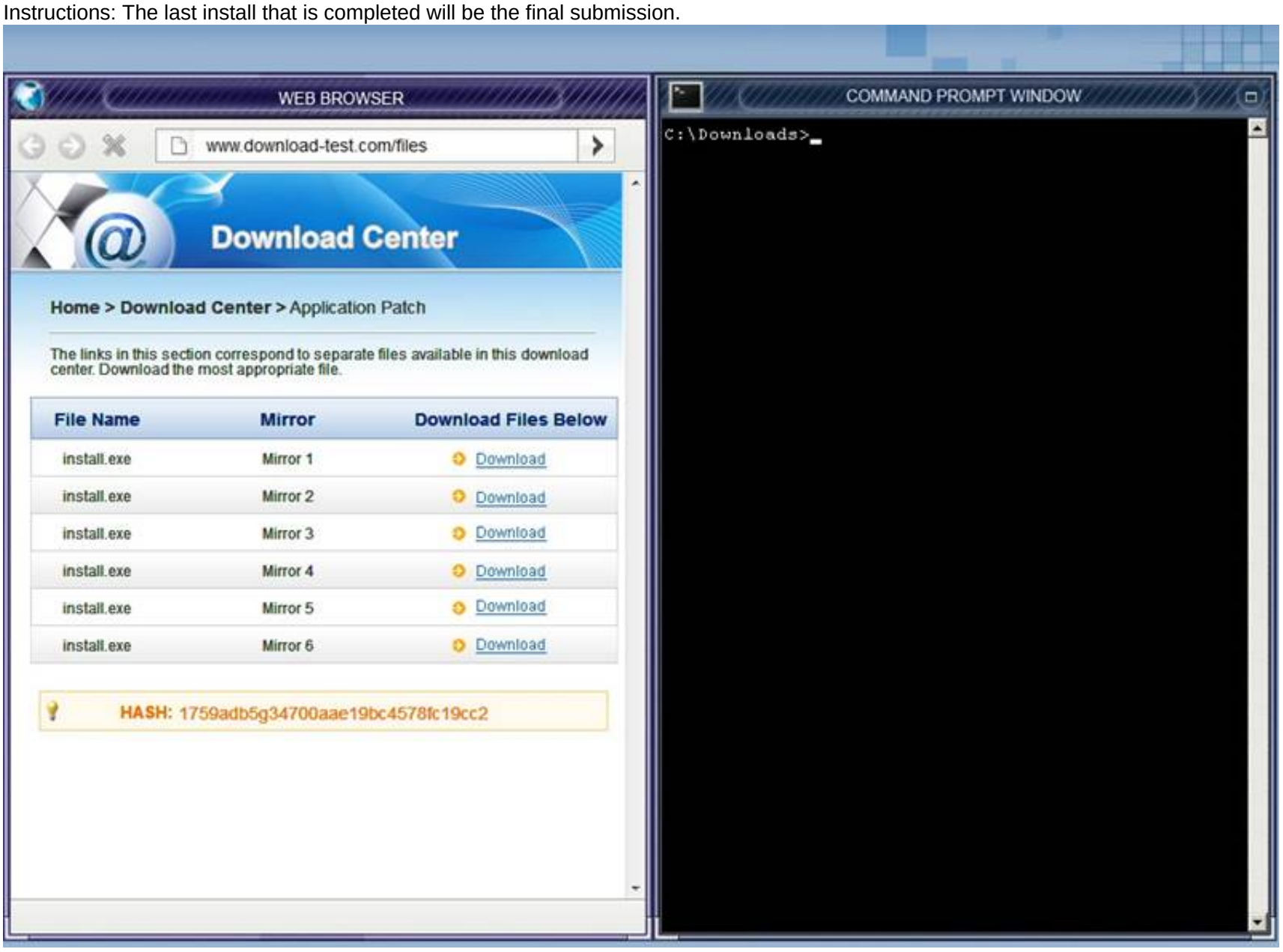
Answer: C

NEW QUESTION 271
- (Topic 2)
A security solutions architect has argued consistently to implement the most secure method of encrypting corporate messages. The solution has been derided as not being cost effective by other members of the IT department. The proposed solution uses symmetric keys to encrypt all messages and is very resistant to unauthorized decryption. The method also requires special handling and security for all key material that goes above and beyond most encryption systems. Which of the following is the solutions architect MOST likely trying to implement?

A. One time pads
B. PKI
C. Quantum cryptography
D. Digital rights management

Answer: A

NEW QUESTION 272
CORRECT TEXT - (Topic 2)
An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner.
Instructions: The last install that is completed will be the final submission.



A.

Answer: Pleasechecktheexplanationpartforfulldetailsonsolution.

NEW QUESTION 277
- (Topic 2)
A company Chief Information Officer (CIO) is unsure which set of standards should govern
the company's IT policy. The CIO has hired consultants to develop use cases to test against various government and industry security standards. The CIO is convinced that there is large overlap between the configuration checks and security controls governing each set of standards. Which of the following selections represent the BEST option for the CIO?

A. Issue a RFQ for vendors to quote a complete vulnerability and risk management solution to the company.
B. Issue a policy that requires only the most stringent security standards be implemented throughout the company.
C. Issue a policy specifying best practice security standards and a baseline to be implemented across the company.

D. Issue a RFI for vendors to determine which set of security standards is best for the company.

Answer: C

NEW QUESTION 279
- (Topic 2)
A security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company's security information and event management server.
Logs: Log 1:
Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packets
Log 2: HTTP://www.company.com/index.php?user=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Log 3:
Security Error Alert
Event ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client
Log 4:
Encoder oe = new OracleEncoder ();
String query = "Select user_id FROM user_data WHERE user_name = ' "
+ oe.encode (req.getParameter("userID")) + " ' and user_password = ' "
+ oe.encode (req.getParameter("pwd")) +" ' ";
Vulnerabilities Buffer overflow SQL injection ACL
XSS
Which of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).

A. Log 1
B. Log 2
C. Log 3
D. Log 4
E. Buffer overflow
F. ACL
G. XSS
H. SQL injection

Answer: BE

NEW QUESTION 280
- (Topic 2)
A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.
Proposal:
External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.
The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?

A. -$30,000
B. $120,000
C. $150,000
D. $180,000

Answer: A

NEW QUESTION 283
- (Topic 2)
A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

A. Remove contact details from the domain name registrar to prevent social engineering attacks.
B. Test external interfaces to see how they function when they process fragmented IP packets.
C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.
D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port
E. scans against external network interfaces.

Answer: B

NEW QUESTION 284
- (Topic 2)
An IT Manager is concerned about errors made during the deployment process for a new model of tablet. Which of the following would suggest best practices and configuration parameters that technicians could follow during the deployment process?

A. Automated workflow
B. Procedure
C. Corporate standard
D. Guideline
E. Policy

Answer: D

NEW QUESTION 287

- (Topic 2)
A small company is developing a new Internet-facing web application. The security requirements are:
1. Users of the web application must be uniquely identified and authenticated.
2. Users of the web application will not be added to the company's directory services.
3. Passwords must not be stored in the code. Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.
B. Use TLS with a shared client certificate for all users.
C. Use SAML with federated directory services.
D. Use Kerberos and browsers that support SAML.

Answer: A

NEW QUESTION 291
- (Topic 2)
The IT Security Analyst for a small organization is working on a customer's system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.
B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.
C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.
D. Refer the issue to management for handling according to the incident response process.

Answer: D

NEW QUESTION 296
- (Topic 2)
A business unit of a large enterprise has outsourced the hosting and development of a new external website which will be accessed by premium customers, in order to speed up the time to market timeline. Which of the following is the MOST appropriate?

A. The external party providing the hosting and website development should be obligated under contract to provide a secure service which is regularly tested (vulnerability and penetration). SLAs should be in place for the resolution of newly identified vulnerabilities and a guaranteed uptime.
B. The use of external organizations to provide hosting and web development services is not recommended as the costs are typically higher than what can be achieved internall
C. In addition, compliance with privacy regulations becomes more complex and guaranteed uptimes are difficult to track and measure.
D. Outsourcing transfers all the risk to the third part
E. An SLA should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.
F. Outsourcing transfers the risk to the third party, thereby minimizing the cost and any legal obligation
G. An MOU should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.

Answer: A

NEW QUESTION 298
- (Topic 2)
An internal development team has migrated away from Waterfall development to use Agile development. Overall, this has been viewed as a successful initiative by the stakeholders as it has improved time-to-market. However, some staff within the security team have
contended that Agile development is not secure. Which of the following is the MOST accurate statement?

A. Agile and Waterfall approaches have the same effective level of security postur
B. They both need similar amounts of security effort at the same phases of development.
C. Agile development is fundamentally less secure than Waterfall due to the lack of formal up-front design and inability to perform security reviews.
D. Agile development is more secure than Waterfall as it is a more modern methodology which has the advantage of having been able to incorporate security best practices of recent years.
E. Agile development has different phases and timings compared to Waterfal
F. Security activities need to be adapted and performed within relevant Agile phases.

Answer: D

NEW QUESTION 303
- (Topic 2)
The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?

A. Race condition
B. Click-jacking
C. Integer overflow
D. Use after free
E. SQL injection

Answer: C

NEW QUESTION 305
- (Topic 2)
A recently hired security administrator is advising developers about the secure integration of a legacy in-house application with a new cloud based processing system. The systems must exchange large amounts of fixed format data such as names, addresses, and phone numbers, as well as occasional chunks of data in

unpredictable formats. The developers want to construct a new data format and create custom tools to parse and process the data. The security administrator instead suggests that the developers:

A. Create a custom standard to define the data.
B. Use well formed standard compliant XML and strict schemas.
C. Only document the data format in the parsing application code.
D. Implement a de facto corporate standard for all analyzed data.

Answer: B

NEW QUESTION 308
- (Topic 2)
ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

A. Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.
B. Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).
C. Organize VM hosts into containers based on security zone and restrict access using an ACL.
D. Require multi-factor authentication when accessing the console at the physical VM host.

Answer: C

NEW QUESTION 312
- (Topic 2)
An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are:
1. Each lab must be on a separate network segment.
2. Labs must have access to the Internet, but not other lab networks.
3. Student devices must have network access, not simple access to hosts on the lab networks.
4. Students must have a private certificate installed before gaining access.
5. Servers must have a private certificate installed locally to provide assurance to the students.
6. All students must use the same VPN connection profile.
Which of the following components should be used to achieve the design in conjunction with directory services?

A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment
B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment
C. IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment
D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Answer: C

NEW QUESTION 317
- (Topic 2)
An IT auditor is reviewing the data classification for a sensitive system. The company has classified the data stored in the sensitive system according to the following matrix:
DATA TYPECONFIDENTIALITYINTEGRITYAVAILABILITY

FinancialHIGHHIGHLOW
Client nameMEDIUMMEDIUMHIGH Client addressLOWMEDIUMLOW
---- AGGREGATEMEDIUMMEDIUMMEDIUM
The auditor is advising the company to review the aggregate score and submit it to senior management. Which of the following should be the revised aggregate score?

A. HIGH, MEDIUM, LOW
B. MEDIUM, MEDIUM, LOW
C. HIGH, HIGH, HIGH
D. MEDIUM, MEDIUM, MEDIUM

Answer: C

NEW QUESTION 318
- (Topic 2)
A project manager working for a large city government is required to plan and build a WAN, which will be required to host official business and public access. It is also anticipated that the city's emergency and first response communication systems will be required to operate across the same network. The project manager has experience with enterprise IT projects, but feels this project has an increased complexity as a result of the mixed business / public use and the critical infrastructure it will provide. Which of the following should the project manager release to the public, academia, and private industry to ensure the city provides due care in considering all project factors prior to building its new WAN?

A. NDA
B. RFI
C. RFP
D. RFQ

Answer: B

NEW QUESTION 322
- (Topic 2)
Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from

infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

A. Install a HIPS on the SIP servers
B. Configure 802.1X on the network
C. Update the corporate firewall to block attacking addresses
D. Configure 802.11e on the network
E. Configure 802.1q on the network

Answer: AD

NEW QUESTION 323
- (Topic 2)
An IT manager is working with a project manager from another subsidiary of the same multinational organization. The project manager is responsible for a new software development effort that is being outsourced overseas, while customer acceptance testing will be performed in house. Which of the following capabilities is MOST likely to cause issues with network availability?

A. Source code vulnerability scanning
B. Time-based access control lists
C. ISP to ISP network jitter
D. File-size validation
E. End to end network encryption

Answer: B

NEW QUESTION 327
- (Topic 2)
An organization recently upgraded its wireless infrastructure to support 802.1x and requires all clients to use this method. After the upgrade, several critical wireless clients fail to
connect because they are only pre-shared key compliant. For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the 802.1x requirement. Which of the following provides the MOST secure method of integrating the non-compliant clients into the network?

A. Create a separate SSID and require the use of dynamic encryption keys.
B. Create a separate SSID with a pre-shared key to support the legacy clients and rotate the key at random intervals.
C. Create a separate SSID and pre-shared WPA2 key on a new network segment and only allow required communication paths.
D. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.

Answer: B

NEW QUESTION 329
- (Topic 3)
A security administrator at a Lab Company is required to implement a solution which will provide the highest level of confidentiality possible to all data on the lab network.
The current infrastructure design includes:
The network is protected with a firewall implementing ACLs, a NIPS device, and secured wireless access points.
Which of the following cryptographic improvements should be made to the current architecture to achieve the stated goals?

A. PKI based authorization
B. Transport encryption
C. Data at rest encryption
D. Code signing

Answer: B

NEW QUESTION 330
- (Topic 3)
An administrator receives reports that the network is running slow for users connected to a certain switch. Viewing the network traffic, the administrator reviews the following:
18:51:59.042108 IP linuxwksta.55467 > dns.company.com.domain: 39462+ PTR? 222.17.4.10.in-addr.arpa. (42)
18:51:59.055732 IP dns.company.com.domain > linuxwksta.55467: 39462 NXDomain 0/0/0 (42)
18:51:59.055842 IP linuxwksta.48287 > dns.company.com.domain: 46767+ PTR? 255.19.4.10.in-addr.arpa. (42)
18:51:59.069816 IP dns.company.com.domain > linuxwksta.48287: 46767 NXDomain 0/0/0 (42)
18:51:59.159060 IP linuxwksta.42491 > 10.4.17.72.iscsi-target: Flags [P.], seq 1989625106:1989625154, ack 2067334822, win 1525, options [nop,nop,TS val 16021424
ecr 215646227], length 48
18:51:59.159145 IP linuxwksta.48854 > dns.company.com.domain: 3834+ PTR? 72.17.4.10.in-addr.arpa. (41)
18:51:59.159314 IP 10.4.17.72.iscsi-target > linuxwksta.42491: Flags [P.], seq 1:49, ack 48, win 124, options [nop,nop,TS val 215647479 ecr 16021424], length 48
18:51:59.159330 IP linuxwksta.42491 > 10.4.17.72.iscsi-target: Flags [.], ack 49, win 1525, options [nop,nop,TS val 16021424 ecr 215647479], length 0
18:51:59.165342 IP dns.company.com.domain > linuxwksta.48854: 3834 NXDomain 0/0/0 (41)
18:51:59.397461 ARP, Request who-has 10.4.16.58 tell 10.4.16.1, length 46 18:51:59.397597 IP linuxwksta.37684 > dns.company.com.domain: 15022+ PTR? 58.16.4.10.in-addr.arpa. (41)
Given the traffic report, which of the following is MOST likely causing the slow traffic?

A. DNS poisoning
B. Improper network zoning
C. ARP poisoning
D. Improper LUN masking

Answer: B

NEW QUESTION 332
- (Topic 3)
A security administrator is redesigning, and implementing a service-oriented architecture to replace an old, in-house software processing system, tied to a corporate sales website. After performing the business process analysis, the administrator decides the services need to operate in a dynamic fashion. The company has also been the victim of data injection attacks in the past and needs to build in mitigation features. Based on these requirements and past vulnerabilities, which of the following needs to be incorporated into the SOA?

A. Point to point VPNs for all corporate intranet users.
B. Cryptographic hashes of all data transferred between services.
C. Service to service authentication for all workflows.
D. Two-factor authentication and signed code

Answer: C

NEW QUESTION 337
- (Topic 3)
A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates. The manager felt the best way to get the changes entered while in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate. The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system. The subordinate did not have authorization to be in the payroll system. Another employee reported the incident to the security team. Which of the following would be the MOST appropriate method for dealing with this issue going forward?

A. Provide targeted security awareness training and impose termination for repeat violators.
B. Block desktop sharing and web conferencing applications and enable use only with approval.
C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.
D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.

Answer: A

NEW QUESTION 341
- (Topic 3)
The Chief Technology Officer (CTO) has decided that servers in the company datacenter should be virtualized to conserve physical space. The risk assurance officer is concerned that the project team in charge of virtualizing servers plans to co-mingle many guest operating systems with different security requirements to speed up the rollout and reduce the number of host operating systems or hypervisors required.
Which of the following BEST describes the risk assurance officer's concerns?

A. Co-mingling guest operating system with different security requirements allows guest OS privilege elevation to occur within the guest OS via shared memory allocation with the host OS.
B. Co-mingling of guest operating systems with different security requirements increases the risk of data loss if the hypervisor fails.
C. A weakly protected guest OS combined with a host OS exploit increases the chance of a successful VMEscape attack being executed, compromising the hypervisor and other guest OS.
D. A weakly protected host OS will allow the hypervisor to become corrupted resulting in
E. data throughput performance issues.

Answer: C

NEW QUESTION 346
- (Topic 3)
A security administrator wants to verify and improve the security of a business process which is tied to proven company workflow. The security administrator was able to improve security by applying controls that were defined by the newly released company security standard. Such controls included code improvement, transport encryption, and interface restrictions. Which of the following can the security administrator do to further increase security after having exhausted all the technical controls dictated by the company's security standard?

A. Modify the company standard to account for higher security and meet with upper management for approval to implement the new standard.
B. Conduct a gap analysis and recommend appropriate non-technical mitigating controls, and incorporate the new controls into the standard.
C. Conduct a risk analysis on all current controls, and recommend appropriate mechanisms to increase overall security.
D. Modify the company policy to account for higher security, adapt the standard accordingly, and implement new technical controls.

Answer: B

NEW QUESTION 350
- (Topic 3)
A corporation has Research and Development (R&D) and IT support teams, each requiring separate networks with independent control of their security boundaries to support department objectives. The corporation's Information Security Officer (ISO) is responsible for providing firewall services to both departments, but does not want to increase the hardware footprint within the datacenter. Which of the following should the ISO consider to provide the independent functionality required by each department's IT teams?

A. Put both departments behind the firewall and assign administrative control for each department to the corporate firewall.
B. Provide each department with a virtual firewall and assign administrative control to the physical firewall.
C. Put both departments behind the firewall and incorporate restrictive controls on each department's network.
D. Provide each department with a virtual firewall and assign appropriate levels of management for the virtual device.

Answer: D

NEW QUESTION 353
- (Topic 3)
Within the company, there is executive management pressure to start advertising to a new target market. Due to the perceived schedule and budget inefficiencies

of engaging a technology business unit to commission a new micro-site, the marketing department is engaging third parties to develop the site in order to meet time-to-market demands. From a security perspective, which of the following options BEST balances the needs between marketing and risk management?

A. The third party should be contractually obliged to perform adequate security activities, and evidence of those activities should be confirmed by the company prior to launch.
B. Outsourcing is a valid option to increase time-to-marke
C. If a security incident occurs, it is not of great concern as the reputational damage will be the third party's responsibility.
D. The company should never outsource any part of the business that could cause a security or privacy inciden
E. It could lead to legal and compliance issues.
F. If the third party has an acceptable record to date on security compliance and is provably faster and cheaper, then it makes sense to outsource in this specific situation.

Answer: A

NEW QUESTION 355
- (Topic 3)
A Physical Security Manager is ready to replace all 50 analog surveillance cameras with IP cameras with built-in web management. The Security Manager has several security guard desks on different networks that must be able to view the cameras without unauthorized people viewing the video as well. The selected IP camera vendor does not have the ability to authenticate users at the camera level. Which of the following should the Security Manager suggest to BEST secure this environment?

A. Create an IP camera network and deploy NIPS to prevent unauthorized access.
B. Create an IP camera network and only allow SSL access to the cameras.
C. Create an IP camera network and deploy a proxy to authenticate users prior to accessing the cameras.
D. Create an IP camera network and restrict access to cameras from a single management host.

Answer: C

NEW QUESTION 358
- (Topic 3)
An administrator is reviewing logs and sees the following entry:
Message: Access denied with code 403 (phase 2). Pattern match "\bunion\b.{1,100}?\bselect\b" at ARGS:$id. [data "union all select"] [severity "CRITICAL"] [tag "WEB_ATTACK"] [tag "WASCTC/WASC-19"] [tag "OWASP_TOP_10/A1"] [tag "OWASP_AppSensor/CIE1"]
Action: Intercepted (phase 2) Apache-Handler: php5-script Which of the following attacks was being attempted?

A. Session hijacking
B. Cross-site script
C. SQL injection
D. Buffer overflow

Answer: C

NEW QUESTION 360
- (Topic 3)
A new web application system was purchased from a vendor and configured by the internal development team. Before the web application system was moved into production, a vulnerability assessment was conducted. A review of the vulnerability assessment report indicated that the testing team discovered a minor security issue with the configuration of the web application. The security issue should be reported to:

A. CISO immediately in an exception report.
B. Users of the new web application system.
C. The vendor who supplied the web application system.
D. Team lead in a weekly report.

Answer: D

NEW QUESTION 364
- (Topic 3)
A financial company implements end-to-end encryption via SSL in the DMZ, and only IPSec in transport mode with AH enabled and ESP disabled throughout the internal network. The company has hired a security consultant to analyze the network infrastructure and provide a solution for intrusion prevention. Which of the following recommendations should the consultant provide to the security administrator?

A. Switch to TLS in the DM
B. Implement NIPS on the internal network, and HIPS on the DMZ.
C. Switch IPSec to tunnel mod
D. Implement HIPS on the internal network, and NIPS on the DMZ.
E. Disable A
F. Enable ESP on the internal network, and use NIPS on both networks.
G. Enable ESP on the internal network, and place NIPS on both networks.

Answer: A

NEW QUESTION 365
- (Topic 3)
A security researcher is about to evaluate a new secure VoIP routing appliance. The appliance manufacturer claims the new device is hardened against all known attacks and several un-disclosed zero day exploits. The code base used for the device is a combination of compiled C and TC/TKL scripts. Which of the following methods should the security research use to enumerate the ports and protocols in use by the appliance?

A. Device fingerprinting
B. Switchport analyzer
C. Grey box testing
D. Penetration testing

Answer: A

NEW QUESTION 366
- (Topic 3)
A company is preparing to upgrade its NIPS at five locations around the world. The three platforms the team plans to test, claims to have the most advanced features and lucrative pricing.
Assuming all platforms meet the functionality requirements, which of the following methods should be used to select the BEST platform?

A. Establish return on investment as the main criteria for selection.
B. Run a cost/benefit analysis based on the data received from the RFP.
C. Evaluate each platform based on the total cost of ownership.
D. Develop a service level agreement to ensure the selected NIPS meets all performance requirements.

Answer: C

NEW QUESTION 369
- (Topic 3)
A data breach has occurred at Company A and as a result, the Chief Information Officer (CIO) has resigned. The CIO's laptop, cell phone and PC were all wiped of data per company policy. A month later, prosecutors in litigation with Company A suspect the CIO knew about the data breach long before it was discovered and have issued a subpoena requesting all the CIO's email from the last 12 months. The corporate retention policy recommends keeping data for no longer than 90 days. Which of the following should occur?

A. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the subpoena request.
B. Inform the litigators that the CIOs information has been deleted as per corporate policy.
C. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the CIO resignation.
D. Restore the CIO's email from an email server backup and provide whatever is available up to the last 12 months from the subpoena date.

Answer: D

NEW QUESTION 370
- (Topic 3)
The Chief Information Officer (CIO) of a technology company is likely to move away from a de-perimeterized model for employee owned devices. This is because there were too many issues with lack of patching, malware incidents, and data leakage due to lost/stolen devices which did not have full-disk encryption. The ‘bring your own computing’ approach was originally introduced because different business units preferred different operating systems and application stacks.
Based on the issues and user needs, which of the following is the BEST recommendation for the CIO to make?

A. The de-perimeterized model should be kept as this is major industry trend and other companies are following this directio
B. Advise that the issues being faced are standard business as usual concerns in a modern IT environment.
C. Update the policy to disallow non-company end-point devices on the corporate networ
D. Develop security-focused standard operating environments (SOEs) for all required operating systems and ensure the needs of each business unit are met.
E. The de-perimeterized model should be kept but update company policies to state that non-company end-points require full disk encryption, anti-virus software, and regular patching.
F. Update the policy to disallow non-company end-point devices on the corporate networ
G. Allow only one type of outsourced SOE to all users as this will be easier to provision, secure, and will save money on operating costs.

Answer: B

NEW QUESTION 374
- (Topic 3)
Which of the following provides the HIGHEST level of security for an integrated network providing services to authenticated corporate users?

A. Point to point VPN tunnels for external users, three-factor authentication, a cold site, physical security guards, cloud based servers, and IPv6 networking.
B. IPv6 networking, port security, full disk encryption, three-factor authentication, cloud based servers, and a cold site.
C. Port security on switches, point to point VPN tunnels for user server connections, two- factor cryptographic authentication, physical locks, and a standby hot site.
D. Port security on all switches, point to point VPN tunnels for user connections to servers, two-factor authentication, a sign-in roster, and a warm site.

Answer: :C

NEW QUESTION 376
- (Topic 3)
A security administrator is conducting network forensic analysis of a recent defacement of the company’s secure web payment server (HTTPS). The server was compromised around the New Year’s holiday when all the company employees were off. The company’s network diagram is summarized below:
The security administrator discovers that all the local web server logs have been deleted. Additionally, the Internal Firewall logs are intact but show no activity from the internal network to the web server farm during the holiday.
Which of the following is true?

A. The security administrator should review the IDS logs to determine the source of the attack and the attack vector used to compromise the web server.
B. The security administrator must correlate the external firewall logs with the intrusion detection system logs to determine what specific attack led to the web server compromise.
C. The security administrator must reconfigure the network and place the IDS between the SSL accelerator and the server farm to be able to determine the cause of future attacks.
D. The security administrator must correlate logs from all the devices in the network

E. diagram to determine what specific attack led to the web server compromise.

Answer: C

NEW QUESTION 379
- (Topic 3)
Staff from the sales department have administrator rights to their corporate standard operating environment, and often connect their work laptop to customer networks when onsite during meetings and presentations. This increases the risk and likelihood of a security incident when the sales staff reconnects to the corporate LAN. Which of the following controls would BEST protect the corporate network?

A. Implement a network access control (NAC) solution that assesses the posture of the laptop before granting network access.
B. Use an independent consulting firm to provide regular network vulnerability assessments and biannually qualitative risk assessments.
C. Provide sales staff with a separate laptop with no administrator access just for sales visits.
D. Update the acceptable use policy and ensure sales staff read and acknowledge the policy.

Answer: A

NEW QUESTION 380
- (Topic 3)
As part of the ongoing information security plan in a large software development company, the Chief Information officer (CIO) has decided to review and update the company's privacy policies and procedures to reflect the changing business environment and business requirements.
Training and awareness of the new policies and procedures has been incorporated into the security awareness program which should be:

A. presented by top level management to only data handling staff.
B. customized for the various departments and staff roles.
C. technical in nature to ensure all development staff understand the procedures.
D. used to promote the importance of the security department.

Answer: B

NEW QUESTION 382
- (Topic 3)
A startup company offering software on demand has hired a security consultant to provide expertise on data security. The company's clients are concerned about data confidentiality. The security consultant must design an environment with data confidentiality as the top priority, over availability and integrity. Which of the following designs is BEST suited for this purpose?

A. All of the company servers are virtualized in a highly available environment sharing common hardware and redundant virtual storag
B. Clients use terminal service access to the shared environment to access the virtualized application
C. A secret key kept by the startup encrypts the application virtual memory and data store.
D. All of the company servers are virtualized in a highly available environment sharing common hardware and redundant virtual storag
E. Clients use terminal service access to the shared environment and to access the virtualized application
F. Each client has a common shared key, which encrypts the application virtual memory and data store.
G. Each client is assigned a set of virtual hosts running shared hardwar
H. Physical storage is partitioned into LUNS and assigned to each clien
I. MPLS technology is used to segment and encrypt each of the client's network
J. PKI based remote desktop with hardware tokens is used by the client to connect to the application.
K. Each client is assigned a set of virtual hosts running shared hardwar
L. Virtual storage is partitioned and assigned to each clien
M. VLAN technology is used to segment each of the client's network
N. PKI based remote desktop access is used by the client to connect to the application.

Answer: C

NEW QUESTION 384
- (Topic 3)
A Chief Information Security Officer (CISO) of a major consulting firm has significantly increased the company's security posture; however, the company is still plagued by data breaches of misplaced assets. These data breaches as a result have led to the compromise of sensitive corporate and client data on at least 25 occasions. Each employee in the company is provided a laptop to perform company business. Which of the following actions can the CISO take to mitigate the breaches?

A. Reload all user laptops with full disk encryption software immediately.
B. Implement full disk encryption on all storage devices the firm owns.
C. Implement new continuous monitoring procedures.
D. Implement an open source system which allows data to be encrypted while processed.

Answer: B

NEW QUESTION 385
- (Topic 3)
A large corporation which is heavily reliant on IT platforms and systems is in financial difficulty and needs to drastically reduce costs in the short term to survive. The Chief Financial Officer (CFO) has mandated that all IT and architectural functions will be outsourced and a mixture of providers will be selected. One provider will manage the desktops for five years, another provider will manage the network for ten years, another provider will be responsible for security for four years, and an offshore provider will perform day to day business processing functions for two years. At the end of each contract the incumbent may be renewed or a new provider may be selected. Which of the following are the MOST likely risk implications of the CFO's business decision?

A. Strategic architecture will be adversely impacted through the segregation of duties between the provider
B. Vendor management costs will remain unchange
C. The risk position of the organization will decline as specialists now maintain the environmen

D. The implementation of security controls and security updates will improv
E. Internal knowledge of IT systems will improve as providers maintain system documentation.
F. Strategic architecture will improve as more time can be dedicated to strateg
G. System stability will improve as providers use specialists and tested processes to maintain system
H. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduced slightl
I. Internal knowledge of IT systems will improve as providers maintain system documentatio
J. The risk position of the organization will remain unchanged.
K. Strategic architecture will not be impacted in the short term, but will be adversely impacted in the long term through the segregation of duties between the provider
L. Vendor management costs will stay the same and the organization's flexibility to react to new market conditions will be improved through best of breed technology implementation
M. Internal knowledge of IT systems will decline over tim
N. The implementation of security controls and security updates will not change.
O. Strategic architecture will be adversely impacted through the segregation of duties between the provider
P. Vendor management costs will increase and the organization's flexibility to react to new market conditions will be reduce
Q. Internal knowledge of IT systems will decline and decrease future platform developmen
R. The implementation of security controls and security updates will take longer as responsibility crosses multiple boundaries.

Answer: D

NEW QUESTION 388
- (Topic 3)
Customer Need:
"We need the system to produce a series of numbers with no discernible mathematical progression for use by our Java based, PKI-enabled, customer facing website."
Which of the following BEST restates the customer need?

A. The system shall use a pseudo-random number generator seeded the same every time.
B. The system shall generate a pseudo-random number upon invocation by the existing Java program.
C. The system shall generate a truly random number based upon user PKI certificates.
D. The system shall implement a pseudo-random number generator for use by corporate customers.

Answer: :B

NEW QUESTION 390
- (Topic 3)
A database administrator comes across the below records in one of the databases during an internal audit of the payment system:
UserIDAddressCredit Card No.Password
jsmith123 fake street55XX-XXX-XXXX-1397Password100 jqdoe234 fake street42XX-XXX-XXXX-202717DEC12
From a security perspective, which of the following should be the administrator's GREATEST concern, and what will correct the concern?

A. Concern: Passwords are stored in plain tex
B. Correction: Require a minimum of 8 alphanumeric characters and hash the password.
C. Concern: User IDs are also usernames, and could be enumerated, thereby disclosing sensitive account informatio
D. Correction: Require user IDs to be more complex by using alphanumeric characters and hash the UserIDs.
E. Concern: User IDs are confidential private informatio
F. Correction: Require encryption of user IDs.
G. Concern: More than four digits within a credit card number are store
H. Correction: Only store the last four digits of a credit card to protect sensitive financial information.

Answer: A

NEW QUESTION 391
- (Topic 3)
About twice a year a switch fails in a company's network center. Under the maintenance contract, the switch would be replaced in two hours losing the business $1,000 per hour. The cost of a spare switch is $3,000 with a 12-hour delivery time and would eliminate downtime costs if purchased ahead of time. The maintenance contract is $1,500 per year.
Which of the following is true in this scenario?

A. It is more cost-effective to eliminate the maintenance contract and purchase a replacement upon failure.
B. It is more cost-effective to purchase a spare switch prior to an outage and eliminate the maintenance contract.
C. It is more cost-effective to keep the maintenance contract instead of purchasing a spare switch prior to an outage.
D. It is more cost-effective to purchase a spare switch prior to an outage and keep the maintenance contract.

Answer: D

NEW QUESTION 394
- (Topic 3)
If a technician must take an employee's workstation into custody in response to an investigation, which of the following can BEST reduce the likelihood of related legal issues?

A. A formal letter from the company's president approving the seizure of the workstation.
B. A formal training and awareness program on information security for all company
C. managers.
D. A screen displayed at log in that informs users of the employer's rights to seize, search, and monitor company devices.
E. A printout of an activity log, showing that the employee has been spending substantial time on non-work related websites.

Answer: C

NEW QUESTION 399
- (Topic 3)
A network administrator notices a security intrusion on the web server. Which of the following is noticed by http://test.com/modules.php?op=modload&name=XForum&file=[hostilejavascript]&fid=2 in the log file?

A. Buffer overflow
B. Click jacking
C. SQL injection
D. XSS attack

Answer: D

NEW QUESTION 401
- (Topic 3)
An organization did not know its internal customer and financial databases were compromised until the attacker published sensitive portions of the database on several popular attacker websites. The organization was unable to determine when, how, or who conducted the attacks but rebuilt, restored, and updated the compromised database server to continue operations.
Which of the following is MOST likely the cause for the organization's inability to determine what really occurred?

A. Too few layers of protection between the Internet and internal network
B. Lack of a defined security auditing methodology
C. Poor intrusion prevention system placement and maintenance
D. Insufficient logging and mechanisms for review

Answer: D

NEW QUESTION 402
- (Topic 3)
A security consultant is called into a small advertising business to recommend which security policies and procedures would be most helpful to the business. The business is comprised of 20 employees, operating off of two shared servers. One server houses employee data and the other houses client data. All machines are on the same local network. Often these employees must work remotely from client sites, but do not access either of the servers remotely. Assuming no security policies or procedures are in place right now, which of the following would be the MOST applicable for implementation? (Select TWO).

A. Password Policy
B. Data Classification Policy
C. Wireless Access Procedure
D. VPN Policy
E. Database Administrative Procedure

Answer: AB

NEW QUESTION 407
- (Topic 3)
A team is established to create a secure connection between software packages in order to list employee's remaining or unused benefits on their paycheck stubs. Which of the following business roles would be MOST effective on this team?

A. Network Administrator, Database Administrator, Programmers
B. Network Administrator, Emergency Response Team, Human Resources
C. Finance Officer, Human Resources, Security Administrator
D. Database Administrator, Facilities Manager, Physical Security Manager

Answer: C

NEW QUESTION 408
- (Topic 3)
An organization has had component integration related vulnerabilities exploited in consecutive releases of the software it hosts. The only reason the company was able to identify the compromises was because of a correlation of slow server performance and an attentive security analyst noticing unusual outbound network activity from the application
servers. End-to-end management of the development process is the responsibility of the applications development manager and testing is done by various teams of programmers. Which of the following will MOST likely reduce the likelihood of similar incidents?

A. Conduct monthly audits to verify that application modifications do not introduce new vulnerabilities.
B. Implement a peer code review requirement prior to releasing code into production.
C. Follow secure coding practices to minimize the likelihood of creating vulnerable applications.
D. Establish cross-functional planning and testing requirements for software development activities.

Answer: D

NEW QUESTION 409
- (Topic 3)
A morphed worm carrying a 0-day payload has infiltrated the company network and is now spreading across the organization. The security administrator was able to isolate the worm communication and payload distribution channel to TCP port 445. Which of the following can the administrator do in the short term to minimize the attack?

A. Deploy the following ACL to the HIPS: DENY - TCP - ANY - ANY – 445.
B. Run a TCP 445 port scan across the organization and patch hosts with open ports.
C. Add the following ACL to the corporate firewall: DENY - TCP - ANY - ANY - 445.
D. Force a signature update and full system scan from the enterprise anti-virus solution.

Answer: A

NEW QUESTION 414
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-002 Practice Exam Features:

* CAS-002 Questions and Answers Updated Frequently

* CAS-002 Practice Questions Verified by Expert Senior Certified Staff

* CAS-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year