Vendor: CompTIA

Exam Code: CAS-001

Exam Name: CompTIA Advanced Security Practitioner

Version: Demo

Q & A: 387

QUESTION 1
Company ENSUREPASS has recently completed the connection of its network to a national high speed private research network. Local businesses in the area are seeking sponsorship from Company ENSUREPASS to connect to the high speed research network by directly connecting through Company ENSUREPASS's network. Company ENSUREPASS's Chief Information Officer (CIO) believes that this is an opportunity to increase revenues and visibility for the company, as well as promote research and development in the area. Which of the following must Company ENSUREPASS require of its sponsored partners in order to document the technical security requirements of the connection?

A. SLA
B. ISA
C. NDA
D. BPA

Correct Answer: B

QUESTION 2
A security analyst at Company A has been trying to convince the Information Security Officer (ISO) to allocate budget towards the purchase of a new intrusion prevention system (IPS) capable of analyzing encrypted web transactions. Which of the following should the analyst provide to the ISO to support the request? (Select TWO).

A. Emerging threat reports
B. Company attack tends
C. Request for Quote (RFQ)
D. Best practices
E. New technologies report

Correct Answer: AB

QUESTION 3
The IT department of a pharmaceutical research company is considering whether the company should allow or block access to social media websites during lunch time. The company is considering the possibility of allowing access only through the company's guest wireless network, which is logically separated from the internal research network. The company prohibits the use of personal devices; therefore, such access will take place from company owned laptops. Which of the following is the HIGHEST risk to the organization?

A. Employee's professional reputation
B. Intellectual property confidentiality loss
C. Downloaded viruses on the company laptops
D. Workstation compromise affecting availability

Correct Answer: B

QUESTION 4
A security audit has uncovered a lack of security controls with respect to employees' network account management. Specifically, the audit reveals that employee's network accounts are not disabled in a timely manner once an employee departs the organization. The company policy states that the network account of an employee should be disabled within eight hours of

termination. However, the audit shows that 5% of the accounts were not terminated until three days after a dismissed employee departs. Furthermore, 2% of the accounts are still active. Which of the following is the BEST course of action that the security officer can take to avoid repeat audit findings?

A. Review the HR termination process and ask the software developers to review the identity management code.
B. Enforce the company policy by conducting monthly account reviews of inactive accounts.
C. Review the termination policy with the company managers to ensure prompt reporting of employee terminations.
D. Update the company policy to account for delays and unforeseen situations in account deactivation.

Correct Answer: C

QUESTION 5
Which of the following is true about an unauthenticated SAMLv2 transaction?

A. The browser asks the SP for a resource. The SP provides the browser with an XHTML format. The browser asks the IdP to validate the user, and then provides the XHTML back to the SP for access.
B. The browser asks the IdP for a resource. The IdP provides the browser with an XHTML format. The browser asks the SP to validate the user, and then provides the XHTML to the IdP for access.
C. The browser asks the IdP to validate the user. The IdP sends an XHTML form to the SP and a cookie to the browser. The browser asks for a resource to the SP, which verifies the cookie and XHTML format for access.
D. The browser asks the SP to validate the user. The SP sends an XHTML form to the IdP. The IdP provides the XHTML form back to the SP, and then the browser asks the SP for a resource.

Correct Answer: A

QUESTION 6
A company which manufactures ASICs for use in an IDS wants to ensure that the ASICs' code is not prone to buffer and integer overflows. The ASIC technology is copyrighted and the confidentiality of the ASIC code design is exceptionally important. The company is required to conduct internal vulnerability testing as well as testing by a third party. Which of the following should be implemented in the SDLC to achieve these requirements?

A. Regression testing by the manufacturer and integration testing by the third party
B. User acceptance testing by the manufacturer and black box testing by the third party
C. Defect testing by the manufacturer and user acceptance testing by the third party
D. White box unit testing by the manufacturer and black box testing by the third party

Correct Answer: D

QUESTION 7
As part of the testing phase in the SDLC, a software developer wants to verify that an application is properly handling user error exceptions. Which of the following is the BEST tool or process for the developer use?

A. SRTM review
B. Fuzzer
C. Vulnerability assessment
D. HTTP interceptor

Correct Answer: B

QUESTION 8
Which of the following is the MOST appropriate control measure for lost mobile devices?

A. Disable unnecessary wireless interfaces such as Bluetooth.
B. Reduce the amount of sensitive data stored on the device.
C. Require authentication before access is given to the device.
D. Require that the compromised devices be remotely wiped.

Correct Answer: D

QUESTION 9
Which of the following is the MOST cost-effective solution for sanitizing a DVD with sensitive information on it?

A. Write over the data
B. Purge the data
C. Incinerate the DVD
D. Shred the DVD

Correct Answer: D

QUESTION 10
A network engineer at Company ENSUREPASS observes the following raw HTTP request:

```
GET /disp_reports.php?SectionEntered=57&GroupEntered=-
1&report_type=alerts&to_date=01-01- 0101&Run=
Run&UserEntered=dsmith&SessionID=5f04189bc&from_date=31-10-
2010&TypesEntered=1 HTTP/1.1
Host: test.example.net
Accept: */*
Accept-LanguagE. en
Connection: close
CookiE. java14=1; java15=1; java16=1; js=1292192278001;
```

Which of the following should be the engineer's GREATEST concern?

A. The HTTPS is not being enforced so the system is vulnerable.
B. The numerical encoding on the session ID is limited to hexadecimal characters, making it susceptible
to a brute force attack.
C. Sensitive data is transmitted in the URL.
D. The dates entered are outside a normal range, which may leave the system vulnerable to a denial

of service attack.

Correct Answer: C

QUESTION 11
Driven mainly by cost, many companies outsource computing jobs which require a large amount of processor cycles over a short duration to cloud providers. This allows the company to avoid a large investment in computing resources which will only be used for a short time. Assuming the provisioned resources are dedicated to a single company, which of the following is the MAIN vulnerability associated with on-demand provisioning?

A. Traces of proprietary data which can remain on the virtual machine and be exploited
B. Remnants of network data from prior customers on the physical servers during a compute job
C. Exposure of proprietary data when in-transit to the cloud provider through IPSec tunnels
D. Failure of the de-provisioning mechanism resulting in excessive charges for the resources

Correct Answer: A

QUESTION 12
A security administrator needs a secure computing solution to use for all of the company's security audit log storage, and to act as a central server to execute security functions from. Which of the following is the BEST option for the server in this scenario?

A. A hardened Red Hat Enterprise Linux implementation running a software firewall
B. Windows 7 with a secure domain policy and smartcard based authentication
C. A hardened bastion host with a permit all policy implemented in a software firewall
D. Solaris 10 with trusted extensions or SE Linux with a trusted policy

Correct Answer: D

QUESTION 13
After implementing port security, restricting all network traffic into and out of a network, migrating to IPv6, installing NIDS, firewalls, spam and application filters, a security administer is convinced that the network is secure. The administrator now focuses on securing the hosts on the network, starting with the servers. Which of the following is the MOST complete list of end-point security software the administrator could plan to implement?

A. Anti-malware/virus/spyware/spam software, as well as a host based firewall and strong, two-factor authentication.
B. Anti-virus/spyware/spam software, as well as a host based IDS, firewall, and strong three-factor authentication.
C. Anti-malware/virus/spyware/spam software, as well as a host based firewall and biometric authentication.
D. Anti-malware/spam software, as well as a host based firewall and strong, three-factor authentication.

Correct Answer: A

QUESTION 14
A security architect is assigned to a major software development project. The software

development team has a history of writing bug prone, inefficient code, with multiple security flaws in every release. The security architect proposes implementing secure coding standards to the project manager. The secure coding standards will contain detailed standards for:

A. error handling, input validation, memory use and reuse, race condition handling, commenting, and preventing typical security problems.
B. error prevention, requirements validation, memory use and reuse, commenting typical security problems,
and testing code standards.
C. error elimination, trash collection, documenting race conditions, peer review, and typical security problems.
D. error handling, input validation, commenting, preventing typical security problems, managing customers,
and documenting extra requirements.

Correct Answer: A

QUESTION 15
A number of security incidents have been reported involving mobile web-based code developed by a consulting company. Performing a root cause analysis, the security administrator of the consulting company discovers that the problem is a simple programming error that results in extra information being loaded into the memory when the proper format is selected by the user. After repeating the process several times, the security administrator is able to execute unintentional instructions through this method. Which of the following BEST describes the problem that is occurring, a good mitigation technique to use to prevent future occurrences, and why it a security concern?

A. Problem: Cross-site scripting
Mitigation Technique. Input validation
Security Concern: Decreases the company's profits and cross-site scripting can enable malicious actors to compromise the confidentiality of network connections or interrupt the availability of the network.
B. Problem: Buffer overflow
Mitigation Technique. Secure coding standards
Security Concern: Exposes the company to liability buffer overflows and can enable malicious actors to compromise the confidentiality/availability of the data.
C. Problem: SQL injection
Mitigation Technique. Secure coding standards
Security Concern: Exposes the company to liability SQL injection and can enable malicious actors to compromise the confidentiality of data or interrupt the availability of a system.
D. Problem: Buffer overflow
Mitigation Technique. Output validation
Security Concern: Exposing the company to public scrutiny buffer overflows can enable malicious actors to interrupt the availability of a system.

Correct Answer: B

QUESTION 16
A security administrator has been conducting a security assessment of Company XYZ for the past two weeks. All of the penetration tests and other assessments have revealed zero flaws in the systems at Company XYZ. However, Company XYZ reports that it has been the victim of numerous security incidents in the past six months. In each of these incidents, the criminals have managed to exfiltrate large volumes of data from the secure servers at the company. Which of the

following techniques should the investigation team consider in the next phase of their assessment in hopes of uncovering the attack vector the criminals used?

A. Vulnerability assessment
B. Code review
C. Social engineering
D. Reverse engineering

Correct Answer: C

QUESTION 17
A security manager at Company ENSUREPASS, needs to perform a risk assessment of a new mobile device which the Chief Information Officer (CIO) wants to immediately deploy to all employees in the company. The product is commercially available, runs a popular mobile operating system, and can connect to IPv6 networks wirelessly. The model the CIO wants to procure also includes the upgraded 160GB solid state hard drive. The producer of the device will not reveal exact numbers but experts estimate that over 73 million of the devices have been sold worldwide. Which of the following is the BEST list of factors the security manager should consider while performing a risk assessment?

A. Ability to remotely wipe the devices, apply security controls remotely, and encrypt the SSD;
the track record of the vendor in publicizing and correcting security flaws in their products;
predicted costs associated with maintaining, integrating and securing the devices.
B. Ability to remotely administer the devices, apply security controls remotely, and remove the SSD;
the track record of the vendor in securely implementing IPv6 with IPSec;
predicted costs associated with securing the devices.
C. Ability to remotely monitor the devices, remove security controls remotely, and decrypt the SSD;
the track record of the vendor in publicizing and preventing security flaws in their products;
predicted costs associated with maintaining, destroying and tracking the devices.
D. Ability to remotely sanitize the devices, apply security controls locally, encrypt the SSD;
the track record of the vendor in adapting the open source operating system to their platform;
predicted costs associated with inventory management, maintaining, integrating and securing the devices.

Correct Answer: A

QUESTION 18
The security administrator is worried about possible SPIT attacks against the VoIP system. Which of the following security controls would MOST likely need to be implemented to detect this type of attack?

A. SIP and SRTP traffic analysis
B. QoS audit on Layer 3 devices
C. IP and MAC filtering logs
D. Email spam filter log

Correct Answer: A

QUESTION 19
The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The network administrator reviews the tickets and compiles the following

information for the security administrator:

```
------
Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0
Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0
Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0
All callers are connected to the same switch and are routed by a router with
five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-
ab-1a
------
```

The security administrator brings a laptop to the finance office, connects it to one of the wall jacks, starts up a network analyzer, and notices the following:

```
09:05:10.937590 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)
09:05:15.934840 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)
09:05:19.931482 arp reply 172.16.34.1 is-at 0:12:3f:f1:da:52 (0:12:3f:f1:da:52)
```

Which of the following can the security administrator determine from the above information?

A. A man in the middle attack is underway - implementing static ARP entries is a possible solution.
B. An ARP flood attack targeted at the router is causing intermittent communication ?implementing IPS is a possible solution.
C. The default gateway is being spoofed - implementing static routing with MD5 is a possible solution.
D. The router is being advertised on a separate network - router reconfiguration is a possible solution.

Correct Answer: A

QUESTION 20
On Monday, the Chief Information Officer (CIO) of a state agency received an e-discovery request for the release of all emails sent and received by the agency board of directors for the past five years. The CIO has contacted the email administrator and asked the administrator to provide the requested information by end of day on Friday. Which of the following has the GREATEST impact on the ability to fulfill the e-discovery request?

A. Data retention policy
B. Backup software and hardware
C. Email encryption software
D. Data recovery procedures

Correct Answer: A

QUESTION 21
A company is evaluating a new marketing strategy involving the use of social networking sites to reach its customers. The marketing director wants to be able to report important company news, product updates, and special promotions on the social websites. After an initial and successful pilot period, other departments want to use the social websites to post their updates as well. The Chief Information Officer (CIO) has asked the company security administrator to document three negative security impacts of allowing IT staff to post work related information on such websites. Which of the following are the major risks the security administrator should report back to the CIO? (Select THREE).

A. Brute force attacks
B. Malware infection
C. DDOS attacks
D. Phishing attacks
E. SQL injection attacks
F. Social engineering attacks

Correct Answer: BDF

QUESTION 22
A telecommunication company has recently upgraded their teleconference systems to multicast. Additionally, the security team has instituted a new policy which requires VPN to access the company's video conference. All parties must be issued a VPN account and must connect to the company's VPN concentrator to participate in the remote meetings. Which of the following settings will increase bandwidth utilization on the VPN concentrator during the remote meetings?

A. IPSec transport mode is enabled
B. ICMP is disabled
C. Split tunneling is disabled
D. NAT-traversal is enabled

Correct Answer: C

QUESTION 23
An Information Security Officer (ISO) has asked a security team to randomly retrieve discarded computers from the warehouse dumpster. The security team was able to retrieve two older computers and a broken MFD network printer. The security team was able to connect the hard drives from the two computers and the network printer to a computer equipped with forensic tools. The security team was able to retrieve PDF files from the network printer hard drive but the data on the two older hard drives was inaccessible. Which of the following should the Warehouse Manager do to remediate the security issue?

A. Revise the hardware and software maintenance contract.
B. Degauss the printer hard drive to delete data.
C. Implement a new change control process.
D. Update the hardware decommissioning procedures.

Correct Answer: D

QUESTION 24
Which of the following precautions should be taken to harden network devices in case of VMEscape?

A. Database servers should be on the same virtual server as web servers in the DMZ network segment.
B. Web servers should be on the same physical server as database servers in the network segment.
C. Virtual servers should only be on the same physical server as others in their network segment.
D. Physical servers should only be on the same WAN as other physical servers in their network.

Correct Answer: C

QUESTION 25
Which of the following should be used with caution because of its ability to provide access to block level data instead of file level data?

A. CIFS
B. NFS
C. iSCSI
D. NAS

Correct Answer: C

QUESTION 26
Which of the following can aid a buffer overflow attack to execute when used in the creation of applications?

A. Secure cookie storage
B. Standard libraries
C. State management
D. Input validation

Correct Answer: B

QUESTION 27
The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the company's internal network. The Chief Information Security Officer (CISO) was told to research and recommend how to secure this device. Which of the following recommendations should be implemented to keep the device from posing a security risk to the company?

A. A corporate policy to prevent sensitive information from residing on a mobile device and anti-virus software.
B. Encryption of the non-volatile memory and a corporate policy to prevent sensitive information from residing on a mobile device.
C. Encryption of the non-volatile memory and a password or PIN to access the device.
D. A password or PIN to access the device and a corporate policy to prevent sensitive information from residing on a mobile device.

Correct Answer: C

QUESTION 28
The Chief Executive Officer (CEO) of a corporation decided to move all email to a cloud computing environment. The Chief Information Security Officer (CISO) was told to research the risk involved in this environment. Which of the following measures should be implemented to minimize the risk of hosting email in the cloud?

A. Remind users that all emails with sensitive information need be encrypted and physically inspect the cloud computing.
B. Ensure logins are over an encrypted channel and obtain an NDA and an SLA from the cloud provider.

C. Ensure logins are over an encrypted channel and remind users to encrypt all emails that contain sensitive information.
D. Obtain an NDA from the cloud provider and remind users that all emails with sensitive information need be encrypted.

Correct Answer: B

QUESTION 29
The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and wants to connect it to the internal network. The Chief Information Security Officer (CISO) was told to research and recommend how to secure this device. Which of the following should be implemented, keeping in mind that the CEO has stated that this access is required?

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

Correct Answer: A

QUESTION 30
The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and connected it to the internal network. The CEO proceeded to download sensitive financial documents through their email. The device was then lost in transit to a conference. The CEO notified the company helpdesk about the lost device and another one was shipped out, after which the helpdesk ticket was closed stating the issue was resolved. This data breach was not properly reported due to insufficient training surrounding which of the following processes?

A. E-Discovery
B. Data handling
C. Incident response
D. Data recovery and storage

Correct Answer: C

QUESTION 31
An employee was terminated and promptly escorted to their exit interview, after which the employee left the building. It was later discovered that this employee had started a consulting business using screen shots of their work at the company which included live customer data. This information had been removed through the use of a USB device. After this incident, it was determined a process review must be conducted to ensure this issue does not recur. Which of the following business areas should primarily be involved in this discussion? (Select TWO).

A. Database Administrator
B. Human Resources
C. Finance
D. Network Administrator
E. IT Management

Correct Answer: BE

QUESTION 32
A technician states that workstations that are on the network in location B are unable to validate certificates, while workstations that are on the main location A's network are having no issues. Which of the following methods allows a certificate to be validated by a single server that returns the validity of that certificate?

A. XACML
B. OCSP
C. ACL
D. CRL

Correct Answer: B

QUESTION 33
A system administrator needs to develop a policy for when an application server is no longer needed. Which of the following policies would need to be developed?

A. Backup policy
B. De-provisioning policy
C. Data retention policy
D. Provisioning policy

Correct Answer: C

QUESTION 34
A web administrator develops a web form for users to respond to the company via a web page. Which of the following should be practiced to avoid a security risk?

A. SQL injection
B. XSS scripting
C. Click jacking
D. Input validation

Correct Answer: D

QUESTION 35
A large enterprise is expanding through the acquisition of a second corporation. Which of the following should be undertaken FIRST before connecting the networks of the newly formed entity?

A. A system and network scan to determine if all of the systems are secure.
B. Implement a firewall/DMZ system between the networks.
C. Develop a risk analysis for the merged networks.
D. Conduct a complete review of the security posture of the acquired corporation.

Correct Answer: C

QUESTION 36

The company is considering issuing non-standard tablet computers to executive management. Which of the following is the FIRST step the security manager should perform?

A. Apply standard security policy settings to the devices.
B. Set up an access control system to isolate the devices from the network.
C. Integrate the tablets into standard remote access systems.
D. Develop the use case for the devices and perform a risk analysis.

Correct Answer: D

QUESTION 37
When authenticating over HTTP using SAML, which of the following is issued to the authenticating user?

A. A symmetric key
B. A PKI ticket
C. An X.509 certificate
D. An assertion ticket

Correct Answer: D

QUESTION 38
Which of the following activities could reduce the security benefits of mandatory vacations?

A. Have a replacement employee run the same applications as the vacationing employee.
B. Have a replacement employee perform tasks in a different order from the vacationing employee.
C. Have a replacement employee perform the job from a different workstation than the vacationing employee.
D. Have a replacement employee run several daily scripts developed by the vacationing employee.

Correct Answer: D

QUESTION 39
A database is hosting information assets with a computed CIA aggregate value of high. The database is located within a secured network zone where there is flow control between the client and datacenter networks. Which of the following is the MOST likely threat?

A. Inappropriate administrator access
B. Malicious code
C. Internal business fraud
D. Regulatory compliance

Correct Answer: A

QUESTION 40
An organization recently upgraded its wireless infrastructure to support WPA2 and requires all clients to use this method. After the upgrade, several critical wireless clients fail to connect because they are only WEP compliant. For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the WPA2 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 WEP key to support the legacy clients and enable detection of rogue APs.
B. Create a separate SSID and WEP key on a new network segment and only allow required communication paths.
C. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.
D. Create a separate SSID and require the use of dynamic WEP keys.

Correct Answer: B

EnsurePass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.
5. **Instant Access to download the Items**

View list of All Exam provided:
http://www.ensurepass.com/certfications?index=A

To purchase Lifetime Full Access Membership click here:
http://www.ensurepass.com/user/register

Valid Discount Code for 2015: JREH-G1A8-XHC6

To purchase the HOT Exams:

Cisco		CompTIA		Oracle	VMWare	IBM
100-101	640-554	220-801	LX0-101	1Z0-051	VCAD510	C2170-011
200-120	200-101	220-802	N10-005	1Z0-052	VCP510	C2180-319
300-206	640-911	BR0-002	SG0-001	1Z0-053	VCP550	C4030-670
300-207	640-916	CAS-001	SG1-001	1Z0-060	VCAC510	C4040-221
300-208	640-864	CLO-001	SK0-003	1Z0-474	VCP5-DCV	RedHat
350-018	642-467	ISS-001	SY0-301	1Z0-482	VCP510PSE	EX200
352-001	642-813	JK0-010	SY0-401	1Z0-485		EX300
400-101	642-832	JK0-801	PK0-003	1Z0-580		
640-461	642-902			1Z0-820		