SANS Security 528 CASP Practice Exam

Number: CAS-001
Passing Score: 750
Time Limit: 60 min
File Version: 1.1

Join us in Washington DC the week of July 22nd for SEC528: SANS Training Program for the CompTIA® New Advanced Security Practitioner Certification™

http://www.sans.org/event/comptia-training-advanced-security-practitioner

Or check out http://ericconrad.com

SANS' Training Program for the new CompTIA® Advanced Security Practitioner Certification™ is designed to prepare you to pass the CASP™ (CompTIA® Advanced Security Practitioner™) exam. The CASP™ exam is an advanced hands-on vendor-neutral exam. In addition to multiple choice questions, the exam tests hand-on knowledge via simulation questions. The simulations may feature the use of command-line encryption tools, applying firewall ACLs, placing secure devices onto a live network map, and much more.

This SANS CompTIA® training provides courseware custom-built to pass the exam; it was designed by SANS instructors who have taken and passed the CASP™ exam. Numerous hands-on exercises will prepare you both for the exam and for the real world.

Exercises include: configuring a live NAS (Network Attached Storage) server, configuring a VoIP server, multiple encryption exercises including applying digital signatures, network design scenarios, configuring and using IPv6, and much more.

Security 528 includes a CASP™ quiz after each section. The instructor will discuss every question and explain the rationale for each right and wrong answer.

Our goal is not memorization. We will teach students how to understand and analyze complex security challenges and determine the right approach: both on the exam and in the real world.

You will learn skills you can apply directly when they you back to work.

SANS' training program for the new CompTIA® Advanced Security Practitioner Certification™ contains the following domains, weighted per the CASP™ exam objectives:

- Enterprise security (40%)
- Risk Management, policy/procedure and legal (24%)
- Research & analysis (14%)
- Integration of computing, communications, and business disciplines (22%)

Exam A

QUESTION 1
You work as a security engineer for SEC528, Inc. The e-commerce aspect of SEC528's web application has been breached and customer financial information appears to have been accessed by the attackers. Based on the information provided, which of the following is the best way to explain the compromise to the CIO?

A. A likely SQL Injection vector was leveraged to breach the database backend of our web application.
B. The confidentiality of customer information seems to have been breached.
C. Our web application's availability has been breached.
D. A claim should be filed with our data reach insurance provider.

Correct Answer: B
Explanation

Explanation/Reference:
From what is stated in the question, we know that confidential customer information has been breached. Explaining this breach of confidentiality to the CIO is incredibly important. Perhaps a SQL Injection vector was used, but that is going beyond what is provided, and likely beyond what the CIO needs to know immediately.

QUESTION 2
Understanding basic risk management is critical for security professionals. Which term is used to explain a weakness in a system or application?

A. Vulnerability
B. Threat
C. Impact
D. Likelihood

Correct Answer: A
Explanation

Explanation/Reference:
Vulnerability is a weakness in an application or system. A threat is something that can cause harm. Impact is the result of a threat taking advantage of a vulnerability. Likelihood demonstrates how often a threat is expected to exploit a vulnerability.

QUESTION 3
In quantitative risk management, Single Loss Expectancy (SLE) is used to quantify what?

A. The amount of data that would be lost if a breach occurred.
B. The percentage of an asset's value that would be lost if a breach occurred.
C. The percentage of data that would be lost if a breach occurred.
D. The amount of financial impact that would result if a breach occurred impacting an asset.

Correct Answer: D
Explanation

Explanation/Reference:
Single Loss Expectancy (SLE) is a term used in quantitative risk management. Understanding the formula for SLE makes the answer obvious: SLE = AV x EF or Single Loss Expectancy = Asset Value x Exposure Factor. Asset Value is how much the asset is worth. Exposure Factor is the percentage of an asset's value that would be lost. So, SLE is a measure of how much money would be lost if a breach occurred.

QUESTION 4
A user has notified SEC528's help desk to report her inability to access internal corporate email after the new

firewall was put into place. After accessing the firewall logs, you notice that her IP address shows the following ports were blocked by the firewall. Which is most likely causing the issue?

A. TCP 25
B. TCP 110
C. UDP 53
D. TCP 3389

Correct Answer: B
Explanation

Explanation/Reference:
TCP port 110 is associated with POP, which is used for client downloads of email. Note, a block of port 995 would be preferable, as this would indicate the client is using an encrypted version of POP. TCP port 25 is also associated with email, but this port is unlikely to impact client downloads of email.

QUESTION 5
SEC528's public facing web server is an IIS system with a vulnerability in the Server Service that is unable to be patched. Your manager is concerned that this system could be exploited from the outside by an attacker using the SMB protocol. SEC528 likely has a significant mitigating factor that decreases the likelihood of exploitation using the method the manager noted. Name the mitigating countermeasure most likely to exist.

A. A NGFW that can block an exploit using advanced signature detection of SMB attacks
B. A traditional firewall that would deny access to the associated ports for SMB
C. An IPS that could employ behavior-based blocking of someone communicating with the web server over SMB
D. An application whitelisting product that would block a web server from communicating over SMB

Correct Answer: B
Explanation

Explanation/Reference:
A simple traditional network based firewall is likely available and also configured to deny access to the ports associated with exploitation of this vulnerability.

QUESTION 6
Client-Side exploitation is the most common means for an attacker to initially gain access within a modern network. The effectiveness of which countermeasure is most significantly diminished by the shift from server-side to client-side exploitation

A. NGFW
B. IPS
C. Antivirus
D. Firewall

Correct Answer: D
Explanation

Explanation/Reference:
The traditional firewall's utility has been substantially impacted by the shift from server to client-side exploitation. The firewall is very effective at reducing the exposure associated with listening services that could be attacked from an external actor. However, the most common vectors for client-side exploitation malicious websites and emails with links/attachments are not easily controlled using traditional firewalls.

QUESTION 7
Which of the following is associated with filtering access on network devices?

A. SSO
B. ACL
C. PKI
D. SSL

Correct Answer: B
Explanation

Explanation/Reference:
ACL - Access Control Lists are associated filtering access on firewalls and other network devices.

QUESTION 8
This refers to directly migrating a physical machine to a virtual machine platform:

A. P2V
B. IaaS
C. VPS
D. PaaS

Correct Answer: A
Explanation

Explanation/Reference:
P2V stands for Physical 2 Virtual, which is a method of converting a physical device into a virtual machine.

QUESTION 9
You read an article about an attacker impacting a host operating system after compromising a guest virtual machine. What term is used to describe this activity?

A. Hypervisor Bypass
B. Co-mingling
C. VMEscape
D. Privilege Escalation

Correct Answer: C
Explanation

Explanation/Reference:
VMEscape is the term associated with breaking out of the supposed confines of a guest virtual machine to impact another guest or the host system.

QUESTION 10
A hypervisor is not a firewall. This statement is most important when considering.

A. Virtual Private Networks
B. Multi-tenant cloud service providers
C. De-provisioning virtual machines
D. Infrastructure as a Service

Correct Answer: B
Explanation

Explanation/Reference:
The fact that a hypervisor is not a firewall has significant implications especially when considering a multi-

tenant could service provider. Other businesses systems situated on the same logical network has serious security implications.

QUESTION 11
Requesting that a service provider offer SEC528, Inc. access to prior penetration test reports, SAS70, or evidence of ISO 27001 certification is an example of what security principle.

A. Due Diligence
B. Due Care
C. Best Practices
D. Attestation

Correct Answer: D
Explanation

Explanation/Reference:
While any of the answer choices could be considered correct, the best answer is attestation. Attestation is trying to get a service provider to "prove" security by showing evidence of 3rd party vetting or adherence to a particular standard.

QUESTION 12
A digitally signed email affords the the recipient guarantee that the sender is the person that actually sent the email and further that the email has not changed. What is the technical/legal term for providing both of these?

A. Non-repudiation
B. Origin Authentication
C. Attestation
D. Integrity

Correct Answer: A
Explanation

Explanation/Reference:
Digital signatures are an example of technical non-repudiation. This means that the sender cannot say that someone else either sent the message or violated the integrity of the message if the digital signature is intact.

QUESTION 13
Hashes are cryptographic one-way transformations that accept an arbitrary input and yield a fixed-length output called a digest. The potential for two different inputs to yield the same digest is referred to as:

A. Collision
B. Diffusion
C. Collusion
D. Dilution

Correct Answer: A
Explanation

Explanation/Reference:
A hash collision occurs when two different inputs yield the same output. Collisions will always be possible given that the input side of a hash algorithm allows for infinite possible inputs while the output side is finite.

QUESTION 14
What is a realtime alternative to CRL?

A. PKI
B. OCSP
C. CA
D. RA

Correct Answer: B
Explanation

Explanation/Reference:
Online Certificate Status Protocol represents a realtime method for requesting certificate revocation information. The CRL, or Certificate Revocation List, is another means of communicating this information.

QUESTION 15
What entails ensuring that if a session key is compromised previously captured communications my not also be decrypted.

A. Separation of Duties
B. Non-repudiation
C. Perfect Forward Secrecy
D. High Entropy

Correct Answer: C
Explanation

Explanation/Reference:
Perfect Forward Secrecy ensures that one symmetric session key becoming compromised does not allow for previously captured communications to also be decrypted.

QUESTION 16
Which are the two protocols that can be used for IPsec VPNs?

A. AH
B. ESP
C. AES
D. SSL

Correct Answer: AB
Explanation

Explanation/Reference:
AH and ESP are the two IPsec VPN protocols. While SSL VPNs are becoming increasingly common, they are unrelated to IPsec VPNs.

QUESTION 17
What type of attack could be detected by noticing an SSL certificate name mismatch warning?

A. sslstrip
B. SSL key compromise
C. CA Compromise
D. SSL MITM

Correct Answer: D
Explanation

Explanation/Reference:

A name mismatch warning could indicate an SSL MITM man-in-the-middle attack. It could, of course, also just be a misconfiguration on the part of the target.

QUESTION 18
Which of these insecure programs/protocols is effectively replaced by SSH?

A. Telnet
B. FTP
C. rlogin
D. rsh

Correct Answer: ABCD
Explanation

Explanation/Reference:
All of these protocols/programs can be replaced by the more security-oriented SSH.

QUESTION 19
Which term indicates the degree of randomness?

A. Cryptography
B. Entropy
C. Steganography
D. PRNG

Correct Answer: B
Explanation

Explanation/Reference:
Entropy describes the amount of randomness. Truly random will have maximum or perfect entropy. Computers attempt to effect random by employing a PRNG Pseudo Random Number Generator.

QUESTION 20
Which password has the most overall entropy?

A. correct horse battery staple
B. Tr0ub4dor&3
C. password
D. 31337

Correct Answer: A
Explanation

Explanation/Reference:
Entropy describes the amount of randomness. While 'Tr0ub4dor&3' has the highest per-character entropy, the longer password 'correct horse battery staple' has higher overall entropy due to its length. See http://xkcd.com/936/.

QUESTION 21
Which of the following is roughly equivalent to an access list for network storage?

A. VSAN Markup
B. LUN Masking
C. FCoE Access
D. HBA Controls

Correct Answer: B
Explanation

Explanation/Reference:
LUN (Logical Unit Number) Masking is a way of implementing access control for networked storage.

QUESTION 22
What technique provides a means for reducing waste storage by eliminating identical chunks of data and replacing them with pointers to one copy of that data?

A. Alternate Data Streams
B. Hierarchical File Systems
C. Compression
D. Deduplication

Correct Answer: D
Explanation

Explanation/Reference:
Deduplication is the technique that eliminates storage waste associated with identical clusters/blocks/files being stored multiple times. It works by replacing the chunk of data with a pointer to a single copy of the duplicated data in question.

QUESTION 23
Which IPv6 prefix indicates an IP address that is internally unique, has a local IPv6 infrastructure available, but will not be publicly routed?

A. ::1/128
B. fc00::/7
C. ff00::/8
D. fe80::/8

Correct Answer: B
Explanation

Explanation/Reference:
fc00::/7 is equivalent to RFC1918 addresses, and exhibits the characteristics described in the question. fe80::/8 could also be used locally and would be unique, but it does not imply a local IPv6 infrastructure.

QUESTION 24
Which trend seeks to reduce capital and possibly operational expenses by allowing employees to leverage their personal computing devices for business purposes?

A. BYOD
B. Cloud Services
C. Insourcing
D. Outsourcing

Correct Answer: A
Explanation

Explanation/Reference:
BYOD, Bring-Your-Own-Device, also referred to as consumerization, is a trend toward allowing employees to leverage their personal devices corporately. Significant challenges exist that relate to security, however, the financial incentives are significant.

QUESTION 25
Identifying and labeling all PHI would be an example of what?

A. Internal Audit
B. Separation of Duties
C. Data Classification
D. Principle of Least Privilege

Correct Answer: C
Explanation

Explanation/Reference:
PHI, Protected Health Information, is data regulated by HIPAA. Identifying and labeling this data would be an example of data classification.

QUESTION 26
Which principle would SEC528, Inc. be employing by requiring multiple individuals' authorizations in order to carry out a particularly critical function?

A. Principle of Least Privilege
B. Minimum Necessary Access
C. Rotation of Duties
D. Separation of Duties

Correct Answer: D
Explanation

Explanation/Reference:
Splitting a critical operation across multiple individuals is an example of Separation of Duties.

QUESTION 27
Employing configuration management and establishing a hardened baseline image demonstrates what security principle?

A. Principle of Least Privilege
B. Separation of Duties
C. Rotation of Duties
D. Prudent Man Rule

Correct Answer: A
Explanation

Explanation/Reference:
Hardened configurations disable functionality that is not business necessary, and therefore can be seen as demonstrating the principle of least privilege.

QUESTION 28
SEC528, Inc. is considering the purchase of a data breach insurance policy. What risk management principle are they considering?

A. Risk Transfer
B. Risk Avoidance
C. Risk Mitigation
D. Risk Elimination

Correct Answer: A
Explanation

Explanation/Reference:
Insurance is the classic example of risk transfer. Purchasing insurance means paying some relatively small consistent fee (premium) to an organization that will in turn accept the risk that your organization is unwilling to accept or cannot effectively mitigate themselves.

QUESTION 29
Prior to accepting a risk, what has most likely occurred?

A. Risk Transfer
B. Risk Mitigation
C. Risk Avoidance
D. Risk Elimination

Correct Answer: B
Explanation

Explanation/Reference:
Risk Mitigation is commonly employed prior to accepting risk. The goal of risk mitigation is to decrease the risk down to an acceptable level.

QUESTION 30
Considering financial matters beyond just acquisition costs is most closely associated with what?

A. TCO
B. ROI
C. ARO
D. ALE

Correct Answer: A
Explanation

Explanation/Reference:
TCO, Total Cost of Ownership, attempts to consider not just the upfront costs associated with an acquisition, but also the costs associated with ongoing maintenance and administration as well as other costs.