Vendor: CompTIA

Exam Code:RC0-C02

Exam Name: CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Version: Demo

QUESTION 1

Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

A. Synchronous copy of data

B. RAID configuration

C. Data de-duplication

D. Storage pool space allocation

E. Port scanning

F. LUN masking/mapping

G. Port mapping

Correct Answer: FG

A logical unit number (LUN) is a unique identifier that designates individual hard disk devices or grouped devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the

management of block storage arrays shared over a storage area network (SAN).

LUN masking subdivides access to a given port. Then, even if several LUNs are accessed through the same port, the server masks can be set to limit each server\\'s access to the appropriate LUNs. LUN masking is typically conducted at the

host bus adapter (HBA) or switch level.

Port mapping is used in `Zoning\\'. In storage networking, Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets to restrict interference, add security, and to simplify management. While a SAN makes available

several devices and/or ports to a single device, each system connected to the SAN should only be allowed access to a controlled subset of these devices/ports. Zoning can be applied to either the switch port a device is connected to OR the

WWN World Wide Name on the host being connected. As port based zoning restricts traffic flow based on the specific switch port a device is connected to, if the device is moved, it will lose access. Furthermore, if a different device is

connected to the port in question, it will gain access to any resources the previous host had access to.

QUESTION 2

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks

B. Job rotation

C. Least privilege

D. Employee termination procedures

Correct Answer: B

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

QUESTION 3

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

Correct Answer: B

The new software development effort is being outsourced overseas. Overseas means a different country and therefore a different time zone. Time-based access control lists allow access to resources only at defined times, for example: during office hours. If time-based access control lists are used at the overseas location while customer acceptance testing will be performed in house, it is likely that the testing would be performed at a time which is not allowed by the time-based access control lists.

Time-based ACLs are types of control lists that allow for network access based on time or day. Its function is similar to that of the extended ACLs. Time-based ACLs is implemented by creating a time range that defines specific times of the day and week. This time range created have to be identified with a specific name and then refer to it by a function. The time restrictions are imposed on the function itself. Time-based ACLs are especially useful when you want to place restriction(s) on inbound or outbound traffic based on the time of day. For example, you might apply time-based ACLs if you wanted to only allow access to the Internet during a particular time of the day or allow access to a particular server only during work hours. The time range relies on the router system clock.

QUESTION 4

The Chief Executive Officer (CEO) has decided to outsource systems which are not core business functions; however, a recent review by Ann, the risk officer, has indicated that core business functions are dependent on the outsourced systems. Ann has requested that the IT department calculates the priority of restoration for all systems and applications under the new business model. Which of the following is the BEST tool to achieve this?

A. Business impact analysis

B. Annualized loss expectancy analysis

C. TCO analysis

D. Residual risk and gap analysis

Correct Answer: A

QUESTION 5

A finance manager says that the company needs to ensure that the new system can "replay" data, up to the minute, for every exchange being tracked by the investment departments. The finance manager also states that the company\\'s transactions need to be tracked against this data for a period of five years for compliance. How would a security engineer BEST interpret the finance manager\\'s needs?

A. Compliance standards

B. User requirements

C. Data elements

D. Data storage

E. Acceptance testing

F. Information digest

G. System requirements

Correct Answer: B

User requirements are used to specify what the USER expects an application or system to do.

In this question, the finance manager has stated what he wants the system to do. Therefore, the answer to this question is `user requirements\\'.

QUESTION 6

A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.

B. Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.

C. Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by business managers.

D. Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Correct Answer: B

Commercially available software packages are often widely available. Huge companies like Microsoft develop software packages that are widely available and in use on most computers. Most companies that develop commercial software make their software available through many commercial outlets (computer stores, online stores etc). Information concerning vulnerabilities is often kept internal to the company that developed the software. The large companies that develop commercial software packages are accountable for the software. Information concerning vulnerabilities being made available could have a huge financial cost to the company in terms of loss of reputation and lost revenues. Information concerning vulnerabilities is often kept internal to the company at least until a patch is available to fix the vulnerability.

QUESTION 7

A system administrator needs to meet the maximum amount of security goals for a new DNS infrastructure. The administrator deploys DNSSEC extensions to the domain names and infrastructure. Which of the following security goals does this meet? (Select TWO).

A. Availability

B. Authentication

C. Integrity

D. Confidentiality

E. Encryption

Correct Answer: BC

DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System. The original design of the Domain Name System (DNS) did not include security; instead it was designed to be a scalable distributed system. The Domain Name System Security Extensions (DNSSEC) attempts to add security, while maintaining backwards compatibility. DNSSEC was designed to protect Internet resolvers (clients) from forged DNS data, such as that created by DNS cache poisoning. It is a set of extensions to DNS, which provide to DNS clients (resolvers): origin authentication of DNS data data integrity (but not availability or confidentiality) authenticated denial of existence.

All answers in DNSSEC are digitally signed. By checking the digital signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server. While protecting IP addresses is the immediate concern for many users, DNSSEC can protect other information such as general-purpose cryptographic certificates stored in CERT records in the DNS.

QUESTION 8

A network engineer wants to deploy user-based authentication across the company\\'s wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user\\'s network access be controlled based on the user\\'s role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML

B. WAYF

C. LDAP

D. RADIUS

E. Shibboleth

F. PKI

Correct Answer: CD

RADIUS is commonly used for the authentication of WiFi connections. We can use LDAP and RADIUS for the authentication of users and devices. LDAP and RADIUS have something in common. They`re both mainly protocols (more than a database) which uses attributes to carry information back and forth. They`re clearly defined in RFC documents so you can expect products from different vendors to be able to function properly together. RADIUS is NOT a database. It\\'s a protocol for asking intelligent questions to a user database. LDAP is just a database. In recent offerings it contains a bit of intelligence (like Roles, Class of Service and so on) but it still is mainly just a rather stupid database. RADIUS (actually RADIUS servers like FreeRADIUS) provide the administrator the tools to not only perform user authentication but also to authorize users based on extremely complex checks and logic. For instance you can allow access on a specific NAS only if the user belongs to a certain category, is a member of a specific group and an outside script allows access. There\\'s no way to perform any type of such complex decisions in a user database.

QUESTION 9

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

Correct Answer: D

In risk assessment a baseline forms the foundation for how an organization needs to increase or enhance its current level of security. This type of assessment will provide Ann with the necessary information to take to management.

QUESTION 10

select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson Which of the following types of attacks is the user attempting?

A. XML injection

B. Command injection

C. Cross-site scripting

D. SQL injection

Correct Answer: D

The code in the question is SQL code. The attack is a SQL injection attack.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application\\'s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION 11

An international shipping company discovered that deliveries left idle are being tampered with. The company wants to reduce the idle time associated with international deliveries by ensuring that personnel are automatically notified when an inbound delivery arrives at the transit dock. Which of the following should be implemented to help the company increase the security posture of its operations?

A. Back office database

B. Asset tracking

C. Geo-fencing

D. Barcode scanner

Correct Answer: C

Mobile device management (MDM) is a type of security software used by an IT department to monitor, manage and secure employees\\' mobile devices that are deployed across multiple mobile service providers and across multiple mobile

operating systems being used in the organization.

A secure container, in a mobile security context, is an authenticated and encrypted area of an employee\\'s device that separates sensitive corporate information from the owner\\'s personal data and apps.

The purpose of containerization is to prevent malware, intruders, system resources or other applications from interacting with the secured application and associated corporate data. Secure data containers are third-party mobile apps. The

container acts as a storage area that is authenticated and encrypted by software and governed by corporate IT security policies. Such apps let IT enforce security policies on the same sensitive business data across different devices, which is

especially useful because native device security capabilities vary.

As BYOD (bring your own device) and consumerization trends have grown, the challenges involved in protecting both corporate data and user privacy have also increased. Containerization is one means of providing administrators with full

control over corporate applications and data without affecting those of the user.

QUESTION 12

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

Correct Answer: D

NMAP works as a port scanner and is used to check if the DNS server is listening on port 53.