WGU C845 - Information Systems Security (SSCP) Testbank

Which of the following is a symmetric algorithm?

A Diffie-Hellman

B RSA

C AES

D HMAC - ✓✓C

How can a user be given the power to set privileges on an object for other users when within a DAC operating system?

A Remove special permissions for the user on the object.

B Grant the user full control over the object.

C Give the user the modify privilege on the object.

D Issue an administrative job label to the user. - ✓✓B

Your company adopts a new end-user security awareness program. This training includes malware introduction, social media issues, password guidelines, data exposure, and lost devices. How often should end users receive this training?

A once a year and upon termination

B upon new hire and once a year thereafter

C upon termination

D twice a year

E upon new hire

F once a year - ✓✓B

What type of event is more likely to trigger the business continuity plan (BCP) rather than the disaster recovery plan (DRP)?

A A port-scanning event against your public servers in the DMZ

B A security breach of an administrator account

C Several users failing to remember their logon credentials

D A level 5 hurricane - ✓✓B

What is the IEEE standard known as port-based network access control which is used to leverage authentication already present in a network to validate clients connecting over hardware devices, such as wireless access points or VPN concentrators?

A IEEE 802.1x

B IEEE 802.15

C IEEE 802.3

D IEEE 802.11 - ✓✓A

Why is change control and management used as a component of software asset management?

A To stop changes from being implemented into an environment

B To oversee the asset procurement process

C To prevent or reduce unintended reduction in security

D To restrict the privileges assigned to compartmentalized administrators - ✓✓C

What is the cost benefit equation?

A [ALE1 - ALE2] - CCM

B AES - CCMP

C total initial risk - countermeasure benefit

D AV x EF x ARO - ✓✓A

What is the best means to restore the most current form of data when a backup strategy is based on starting each week off with a full backup followed by a daily differential?

A Restore the initial week's full backup and then the last differential backup before the failure.

B Restore only the last differential backup.

C Restore the initial week's full backup and then each differential backup up to the failure.

D Restore the last differential backup and then the week's full backup. - ✓✓A

Which of the following is not considered an example of a non-discretionary access control system?

A MAC

B ACL

C ABAC

D RBAC - ✓✓B

How should countermeasures be implemented as part of the recovery phase of incident response?

A During next year's security review

B Based on the lowest cost among available options

C As defined by the current security policy

D As determined by the violation that occurred - ✓✓D

Remote control malware was found on a client device, and an unknown attacker was manipulating the network from afar. The attack resulted in the network switches reverting to flooding mode, thereby enabling the attacker to eavesdrop on a significant portion of network communications. After reviewing IDS and traffic logs, you determine that this was accomplished by an attack utility which generated a constant Ethernet frames with random source MAC addresses. What can be done to prevent this attack from occurring in the future?

A Restrict access to DHCP.

B Use a static HOSTS file.

C Use MAC limiting on the switch ports.

D Implement an ARP monitor. - ✓✓C

How is quantitative risk analysis performed?

A Through the Delphi technique

B With scenario-based assessments

C Using calculations

D Via employee interviews - ✓✓C

What special component on a motherboard can be used to securely store the encryption key for whole drive encryption?

A CMOS

B RAM

C TPM

D CPU - ✓✓C

When is it appropriate to contact law enforcement when an organization experiences a security breach?

A If a violation is more severe than just breaking company policy rules

B If a breach of security occurs

C If a tolerable or accepted risk is realized

D If an insider uses another employee's credentials - ✓✓A

What is the name of a cryptographic attack based on a database of pre-computed hash values and the original plaintext values?

A Brute force attack

B Rainbow table attack

C Frequency analysis

D Chosen plaintext attack - ✓✓B

What is the purpose of a Security Information and Event Management (SIEM) product?

A To provide real-time logging and analysis of security events

B To define the requirements of security procedures

C To provide event planning guidance for holding industry conferences

D To improve employee security training - ✓✓A

How does salting passwords reduce the likelihood that a password cracking attack will be successful?

A It prevents automated attacks.

B It forces the attacker to focus on one account at a time.

C It triggers an account lockout after a fixed number of false attempts.

D It increases the work load required to become successful. - ✓✓D

Which of the following clearance levels or classification labels is not generally used in a government- or military-based MAC scheme?

A Unclassified

B Confidential

C Top Secret

D Proprietary - ✓✓D

You are starting a new website. You want to quickly allow users to begin using your site without having the hassle of creating a new user account. You set up a one-way trust federated access link from your website to the three major social networks. Why should you use a one-way trust in this configuration rather than a two-way trust in this scenario?

A A one-way trust allows your website to trust the user accounts of the social networks without requiring the social networks to trust your website.

B Two-way trusts are only valid in private networks and cannot be used across the Internet.

C A one-way trust allows your website to access the file storage of the social networks.