Vendor: EC-Council

Exam Code: 112-51

Exam Name: Network Defense Essentials Exam

Version: DEMO

QUESTION 1
Which of the following algorithms uses a sponge construction where message blocks are XORed into the initial bits of the state that the algorithm then invertible permutes?

A. MD5
B. SHA-2
C. SHA-3
D. MD6

Answer: C
Explanation:
SHA-3 is the algorithm that uses a sponge construction where message blocks are XORed into the initial bits of the state that the algorithm then invertible permutes. SHA-3 is a family of cryptographic hash functions that was standardized by NIST in 2015 as a successor to SHA-2. SHA-3 is based on the Keccak algorithm, which won the NIST hash function competition in 20. SHA-3 uses a sponge construction, which is a simple iterated construction that can produce variable-length output from a fixed-length permutation. The sponge construction operates on a state of b bits, which is divided into two sections: the bitrate r and the capacity c. The sponge construction has two phases: the absorbing phase and the squeezing phase. In the absorbing phase, the input message is padded and divided into blocks of r bits. Each block is XORed into the first r bits of the state, and then the state is transformed by the permutation function f. This process continues until all the input blocks are processed. In the squeezing phase, the output is generated by repeatedly applying the permutation function f to the state and extracting the first r bits as output blocks. The output can be truncated to the desired length. SHA-3 uses a permutation function f that is based on a round function that consists of five steps: theta, rho, pi, chi, and iota. These steps perform bitwise operations, rotations, permutations, and additions on the state. The permutation function f is invertible, meaning that it can be reversed to obtain the previous state. SHA-3 has four variants with different output lengths: SHA3-224, SHA3-256, SHA3-384, and SHA3-5. SHA-3 also supports two additional modes: SHAKE128 and SHAKE256, which are extendable-output functions that can produce arbitrary-length output.

QUESTION 2
Below are the various steps involved in the creation of a data retention policy.

1.Understand and determine the applicable legal requirements of the organization
2.Ensure that all employees understand the organization's data retention policy
3.Build a data retention policy development team
4.Identify and classify the data to be included in the data retention policy
5.Develop the data retention policy

Identify the correct sequence of steps involved.

A. 3 -- >2 -- >5 -- >4 -- >1
B. 3 -- >1 -- >4 -- >5 -- >2
C. 1 -- >3 -- >4 -- >2 -- >5
D. 1 -- >5 -- >4 -- >2 -- >3

Answer: B
Explanation:
The correct sequence of steps involved in the creation of a data retention policy is 3 -> 1 -> 4 -> 5 ->2. This is based on the following description of the data retention policy creation process from the web search results:
Build a team: To design a data retention policy, you need a team of industry experts, such as legal, IT, compliance, and business representatives, who can contribute their knowledge and

perspectives to the policy. The team should have a clear leader who can coordinate the tasks and communicate the goals and expectations.
Determine legal requirements: The team should research and understand the applicable legal and regulatory requirements for data retention that affect the organization, such as GDPR, HIPAA, PCI DSS, etc. The team should also consider any contractual obligations or industry standards that may influence the data retention policy.
Identify and classify the data: The team should inventory and categorize all the data that the organization collects, stores, and processes, based on their function, subject, or type. The team should also assess the value, risk, and sensitivity of each data category, and determine the appropriate retention period, format, and location for each data category. Develop the data retention policy: The team should draft the data retention policy document that outlines the purpose, scope, roles, responsibilities, procedures, and exceptions of the data retention policy. The policy should be clear, concise, and consistent, and should reflect the legal and business requirements of the organization. The policy should also include a data retention schedule that specifies the retention period and disposition method for each data category. Ensure that all employees understand the organization's data retention policy: The team should communicate and distribute the data retention policy to all the relevant employees and stakeholders, and provide training and guidance on how to comply with the policy. The team should also monitor and enforce the policy, and review and update the policy regularly to reflect any changes in the legal or business environment.

QUESTION 3
Cibel.org, an organization, wanted to develop a web application for marketing its products to the public. In this process, they consulted a cloud service provider and requested provision of development tools, configuration management, and deployment platforms for developing customized applications.
Identify the type of cloud service requested by Cibel.org in the above scenario.

A. Security-as-a-service (SECaaS)
B. Platform-as-a-service
C. Infrastructure-as-a-service {laaS)
D. Identity-as-a-service {IDaaS)

Answer: B
Explanation:
The type of cloud service requested by Cibel.org in the above scenario is Platform-as-a-service (PaaS). PaaS is a cloud-based service that delivers a range of developer tools and deployment capabilities. PaaS provides a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining and managing applications. PaaS customers do not need to install, configure, or manage the underlying infrastructure, such as servers, storage, network, or operating system. Instead, they can focus on the application development and deployment process, using the tools and services provided by the cloud service provider. PaaS solutions support cloud-native development technologies, such as microservices, containers, Kubernetes, serverless computing, that enable developers to build once, then deploy and manage consistently across private cloud, public cloud and on-premises environments. PaaS also offers features such as scalability, availability, security, backup, and monitoring for the applications. PaaS is suitable for organizations that want to develop customized applications without investing in or maintaining the infrastructure.

QUESTION 4
Ben, a computer user, applied for a digital certificate. A component of PKI verifies Ben's identity using the credentials provided and passes that request on behalf of Ben to grant the digital certificate.

Which of the following PKI components verified Ben as being legitimate to receive the certificate?

A. Certificate authority (CA)
B. Registration authority {RA)
C. Certificate directory
D. Validation authority (VA)

Answer: B
Explanation:
The PKI component that verified Ben as being legitimate to receive the certificate is the registration authority (RA). An RA is an entity that is responsible for identifying and authenticating certificate applicants, approving or rejecting certificate applications, and initiating certificate revocations or suspensions under certain circumstances. An RA acts as an intermediary between the certificate authority (CA) and the certificate applicant, and performs the necessary checks and validations before forwarding the request to the CA. The CA is the entity that signs and issues the certificates, and maintains the certificate directory and the certificate revocation list. A certificate directory is a repository of issued certificates that can be accessed by users or applications to verify the validity and status of a certificate. A validation authority (VA) is an entity that provides online certificate validation services, such as OCSP or SCVP, to verify the revocation status of a certificate in real time.

QUESTION 5
George, a certified security professional, was hired by an organization to ensure that the server accurately responds to customer requests. In this process, George employed a security solution to monitor the network traffic toward the server. While monitoring the traffic, he identified attack signatures such as SYN flood and ping of death attempts on the server. Which of the following categories of suspicious traffic signature has George identified in the above scenario?

A. Informational
B. Reconnaissance
C. Unauthorized access
D. Denial-of-service (DoS)

Answer: D
Explanation:
Denial-of-service (DoS) is the category of suspicious traffic signature that George identified in the above scenario. DoS signatures are designed to detect attempts to disrupt or degrade the availability or performance of a system or network by overwhelming it with excessive or malformed traffic. SYN flood and ping of death are examples of DoS attacks that exploit the TCP/IP protocol to consume the resources or crash the target server. A SYN flood attack sends a large number of TCP SYN packets to the target server, without completing the three-way handshake, thus creating a backlog of half-open connections that exhaust the server's memory or bandwidth. A ping of death attack sends a malformed ICMP echo request packet that exceeds the maximum size allowed by the IP protocol, thus causing the target server to crash or reboot. DoS attacks can cause serious damage to the organization's reputation, productivity, and revenue, and should be detected and mitigated as soon as possible.

QUESTION 6
James was recruited as security personnel in an organization and was instructed to secure the organization's infrastructure from physical threats. To achieve this, James installed CCTV systems near gates, reception, hallways, and workplaces to capture illicit activities inside the premises, identify activities that need attention, collect images as evidence, and aid in an alarm system. Identify the type of physical security control implemented by James in the above

scenario.

A. Video surveillance
B. Fire-fighting systems
C. Lighting system
D. Physical barriers

Answer: A

QUESTION 7
Below are various authentication techniques.

1.Retina scanner
2.One-time password
3.DNA
4.Voice recognition

Identify the techniques that fall under biometric authentication.

A. 1, 3, and 4
B. 1, 2, and 3
C. 2, 3, and 4
D. 1, 2, and 4

Answer: A
Explanation:
Biometric authentication is a type of authentication that uses the physical or behavioral characteristics of a person to verify their identity. Biometric authentication is more secure and convenient than other methods such as passwords or tokens, as biometric traits are unique, hard to forge, and easy to use. Some examples of biometric authentication techniques are retina scanner, DNA, and voice recognition. Retina scanner uses a low-intensity light beam to scan the pattern of blood vessels at the back of the eye, which is unique for each individual. DNA uses the genetic code of a person to match their identity, which is the most accurate and reliable biometric technique. Voice recognition uses the sound and pitch of a person's voice to verify their identity, which is influenced by factors such as anatomy, physiology, and psychology. These techniques fall under biometric authentication, as they use the physical or behavioral traits of a person to authenticate them.

QUESTION 8
Kelly, a cloud administrator at TechSol Inc., was instructed to select a cloud deployment model to secure the corporate data and retain full control over the data. Which of the following cloud deployment models helps Kelly in the above scenario?

A. Public cloud
B. Multi cloud
C. Community cloud
D. Private cloud

Answer: D
Explanation:
A private cloud is a cloud deployment model that is exclusively used by a single organization and is hosted either on-premises or off-premises by a third-party provider. A private cloud offers the

highest level of security and control over the data and resources, as the organization can customize the cloud infrastructure and services according to its needs and policies. A private cloud also ensures better performance and availability, as the organization does not share the cloud resources with other users. A private cloud is suitable for organizations that have sensitive or confidential data, strict compliance requirements, or high demand for scalability and flexibility. A private cloud can help Kelly secure the corporate data and retain full control over the data in the above scenario.

QUESTION 9
Steve was sharing his confidential file with John via an email that was digitally signed and encrypted. The digital signature was made using the "Diffie-Hellman (X9.42) with DSS" algorithm, and the email was encrypted using triple DES.
Which of the following protocols employs the above features to encrypt an email message?

A. S/MIME
B. EAP
C. RADIUS
D. TACACS+

Answer: A
Explanation:
S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that provides security services for email messages, such as encryption, digital signature, authentication, and integrity. S/MIME is based on the MIME standard, which defines the format and structure of email messages. S/MIME uses public-key cryptography to encrypt and decrypt the message content and to sign and verify the message sender. S/MIME supports various algorithms for encryption and digital signature, such as Diffie-Hellman, DSS, RSA, and triple DES. S/MIME is widely used for secure email communication in various applications and platforms, such as Outlook, Gmail, and Thunderbird. S/MIME is the protocol that employs the features mentioned in the question, namely Diffie-Hellman (X9.42) with DSS for digital signature and triple DES for encryption.

QUESTION 10
Joseph, a security professional, was instructed to secure the organization's network. In this process, he began analyzing packet headers to check whether any indications of source and destination IP addresses and port numbers are being changed during transmission. Identify the attack signature analysis technique performed by Joseph in the above scenario.

A. Composite-signature-based analysis
B. Context-based signature analysis
C. Content-based signature analysis
D. Atomic-signature-based analysis

Answer: D
Explanation:
Atomic-signature-based analysis is a type of attack signature analysis technique that uses a single characteristic or attribute of a packet header to identify malicious traffic. Atomic signatures are simple and fast to match, but they can also generate false positives or miss some attacks. Some examples of atomic signatures are source and destination IP addresses, port numbers, protocol types, and TCP flags. Atomic-signature-based analysis is the technique performed by Joseph in the above scenario, as he analyzed packet headers to check whether any indications of source and destination IP addresses and port numbers are being changed during transmission.

QUESTION 11
Kevin logged into a banking application with his registered credentials and tried to transfer some amount from his account to Flora's account. Before transferring the amount to Flora's account, the application sent an OTP to Kevin's mobile for confirmation. Which of the following authentication mechanisms is employed by the banking application in the above scenario?

A. Biometric authentication
B. Smart card authentication
C. Single sign-on (SSO) authentication
D. Two-factor authentication

Answer: D
Explanation:
Two-factor authentication (2FA) is a type of authentication that requires users to provide two or more forms of verification to access an online account. 2FA is a multi-layered security measure designed to prevent hackers from accessing user accounts using stolen or shared credentials. 2FA typically combines something the user knows (such as a password or PIN), something the user has (such as a phone or a token), and/or something the user is (such as a fingerprint or a face scan). In the above scenario, the banking application employs 2FA by asking Kevin to enter his registered credentials (something he knows) and an OTP sent to his mobile (something he has) before transferring the amount to Flora's account.

QUESTION 12
Messy, a network defender, was hired to secure an organization's internal network. He deployed an IDS in which the detection process depends on observing and comparing the observed events with the normal behavior and then detecting any deviation from it. Identify the type of IDS employed by Messy in the above scenario.

A. Signature-based
B. Stateful protocol analysis
C. Anomaly-based
D. Application proxy

Answer: C
Explanation:
Anomaly-based IDS is a type of IDS that detects intrusions by comparing the observed network events with a baseline of normal behavior and identifying any deviation from it. Anomaly-based IDS can detect unknown or zero-day attacks that do not match any known signature, but they can also generate false positives due to legitimate changes in network behavior. Anomaly-based IDS can use various techniques to model the normal behavior, such as statistical analysis, machine learning, or artificial intelligence. Anomaly-based IDS is the type of IDS employed by Messy in the above scenario, as he deployed an IDS that depends on observing and comparing the observed events with the normal behavior and then detecting any deviation from it.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14