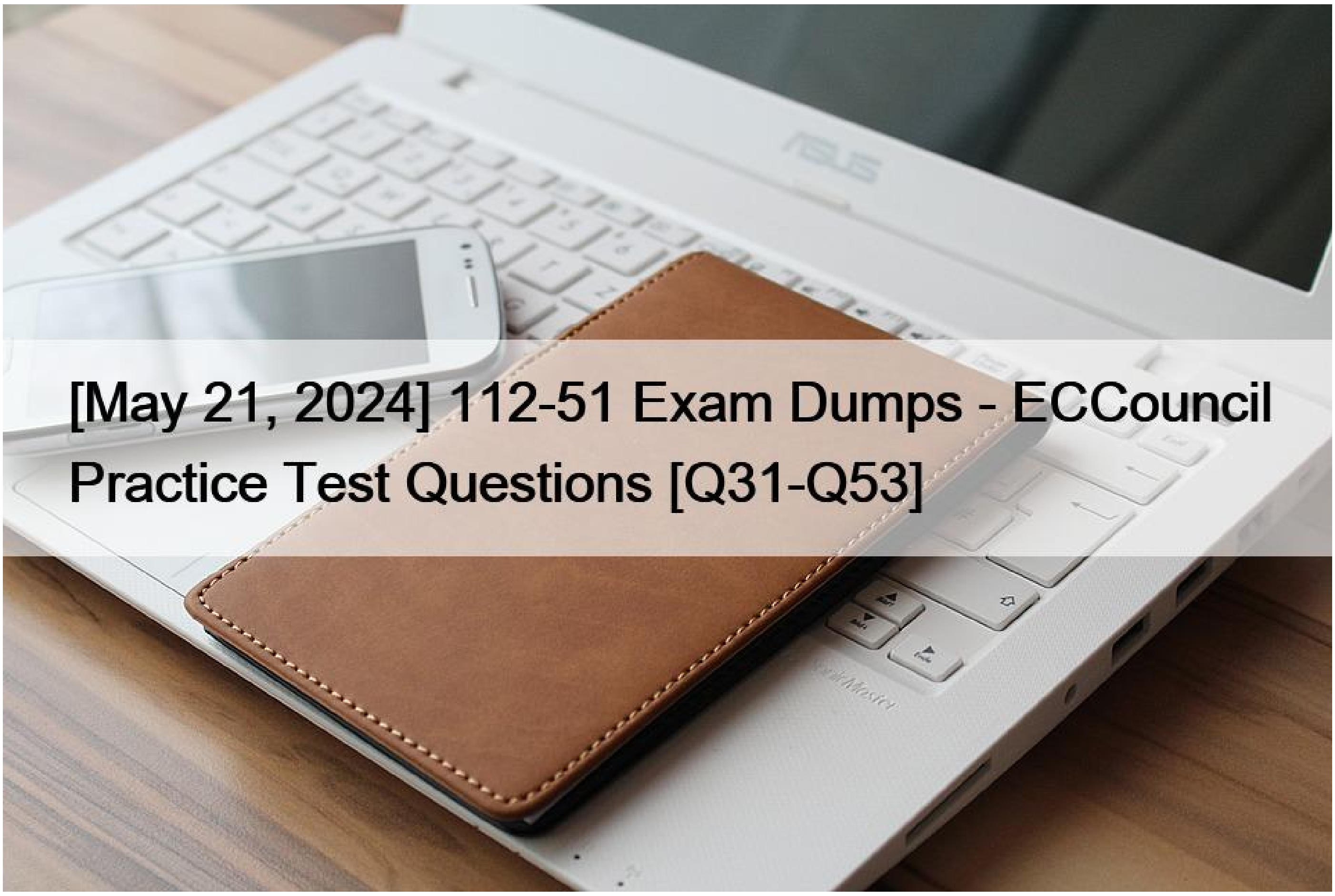
[May 21, 2024 112-51 Exam Dumps - ECCouncil Practice Test Questions [Q31-Q53



[May 21, 2024] 112-51 Exam Dumps - ECCouncil Practice Test Questions
New Real 112-51 Exam Dumps Questions

QUESTION 31

Joseph, a cloud administrator, was recruited for the management and deployment of the software containers. As part of his job, Joseph employed an automated solution that converts images into containers, deploys them to the hosts, and further monitors container workflow from a single location.

Identify the solution employed by Joseph in the above scenario.
* Port scanners
* Orchestrators
* Network monitors
* Sniffers
Orchestrators are tools that automate container deployment, administration, and scaling tasks. They allow you to reliably manage fleets of hundreds or thousands of containers in production environments. Orchestrators simplify container admin by letting you think in terms of application components instead of individual containers. They&#8217;re able to take control of all your

app&#8217;s requirements, including config values, secrets, and network services. Orchestrators are the solution employed by Joseph in the above scenario, as he used an automated solution that converts images into containers, deploys them to the hosts, and further monitors container workflow from a single location.References:

* 13 Most Useful Container Orchestration Tools in 2024 &#8211; Spacelift

* Network Defense Essentials &#8211; CERT &#8211; EC-Council- Module 6: Virtualization and Cloud Computing

QUESTION 32

Identify the technique through which mobile application marketers utilize the user&#8217;s location to gather sensitive data and know about users&#8217; offline activities from the location data.
* Containerization
* Push notification
* Full device encryption
* Geofencing
Geofencing is a technique that uses the user&#8217;s location data to create a virtual boundary around a specific geographic area. Mobile applications can use geofencing to trigger certain actions or notifications when the user enters or exits the defined area. For example, a mobile application can send a push notification to the user when they are near a store or a restaurant. However, geofencing can also be used by marketers to gather sensitive data and know about users&#8217; offline activities from the location data. For instance, a mobile application can track the user&#8217;s movements and preferences based on the places they visit and the time they spend there.This can help marketers to target the user with personalized ads and offers, but it can also pose a threat to the user&#8217;s privacy and security12.References:Network Defense Essentials &#8211; EC-Council Learning,Geofencing: What Is It and How Does It Work?

QUESTION 33

Jay, a network administrator, was monitoring traffic flowing through an IDS. Unexpectedly, he received an event triggered as an alarm, although there is no active attack in progress.

Identify the type of IDS alert Jay has received in the above scenario.
* True negative alert
* False positive alert
* True positive alert
* False negative alert
A false positive alert is a type of IDS alert that occurs when the IDS mistakenly identifies benign or normal traffic as malicious or suspicious, and triggers an alarm, although there is no active attack in progress. A false positive alert can be caused by various factors, such as misconfigured IDS rules, outdated signatures, network anomalies, or legitimate traffic that resembles attack patterns. A false positive alert can waste the time and resources of the security team, as they have to investigate and verify the alert, and also reduce the trust and confidence in the IDS. A false positive alert can be reduced by tuning and updating the IDS, filtering out irrelevant traffic, and using multiple detection methods. A false positive alert is the type of IDS alert Jay has received in the above scenario, as he received an event triggered as an alarm, although there is no active attack in progress.References:

* False Positive Alert- Week 10: Intrusion Detection and Prevention Systems

* What is a False Positive in Cybersecurity?

* How to Reduce False Positives in Intrusion Detection Systems

QUESTION 34

Robert, an ISP, was instructed to provide network connectivity to all areas even if some locations are inaccessible to capture direct signals from wireless access points. In this process, Robert used a wireless network component that takes a signal from one access point and boosts its signal strength to create a new network.

Identify the component of the wireless network employed by Robert in the above scenario.
* Mobile hotspot
* Wireless bridge
* Wireless NIC
* Wireless repeater
A wireless repeater is a wireless network component that takes a signal from one access point and boosts its signal strength to create a new network. A wireless repeater can extend the range of a wireless network by repeating the signal from the original access point. This way, the wireless repeater can provide network connectivity to areas that are inaccessible to capture direct signals from the access point.In the scenario, Robert used a wireless repeater to provide network connectivity to all areas12.References:Network Defense Essentials &#8211; EC-Council Learning,Understanding the Wireless Network Components

QUESTION 35

Clark, a security team member of an organization, was instructed to secure the premises from unauthorized entries. In this process, Clark implemented security controls that allow employees to enter the office only after scanning their badges or fingerprints.

Which of the following security controls has Clark implemented in the above scenario?
* Administrative security controls
* Technical security controls
* Physical security controls
* System access controls
Physical security controls are security measures that prevent or deter unauthorized physical access to a facility, resource, or information. Physical security controls include locks, doors, gates, fences, guards, cameras, alarms, sensors, biometrics, and badges. Physical security controls protect the network and its components from theft, damage, sabotage, or natural disasters. Clark implemented physical security controls in the above scenario, as he installed security controls that allow employees to enter the office only after scanning their badges or fingerprints.References:

* Understanding the Various Types of Physical Security Controls- Week 4: Network Security Controls:

Physical Controls

* The Role of Physical Security in Maintaining Network Security

* Physical Security: Planning, Measures & Examples + PDF

QUESTION 36

Clark, a security professional, was instructed to monitor and continue the backup functions without interrupting the system or application services. In this process, Clark implemented a backup mechanism that dynamically backups the data even if the system or application resources are being used.

Which of the following types of backup mechanisms has Clark implemented in the above scenario?
* Full backup
* Offline backup
* Cold backup

* Hot backup
A hot backup is a type of backup mechanism that dynamically backs up the data even if the system or application resources are being used. A hot backup does not require the system or application to be shut down or paused during the backup process, and it allows the users to access the data while the backup is in progress.

A hot backup ensures that the backup is always up to date and consistent with the current state of the data, and it minimizes the downtime and disruption of the system or application services. A hot backup is suitable for systems or applications that have high availability and performance requirements, such as databases, web servers, or email servers. A hot backup is the type of backup mechanism that Clark implemented in the above scenario, as he performed a backup that dynamically backs up the data even if the system or application resources are being used.References:

* Hot Backup- Week 5: Data Security

* Hot Backup vs. Cold Backup: What&#8217;s the Difference?

* Network Defense Essentials (NDE) | Coursera- Module 5: Data Security

QUESTION 37

Steve was sharing his confidential file with John via an email that was digitally signed and encrypted. The digital signature was made using the &#8220;Diffie-Hellman (X9.42) with DSS&#8221; algorithm, and the email was encrypted using triple DES.

Which of the following protocols employs the above features to encrypt an email message?
* S/MIME
* EAP
* RADIUS
* TACACS+
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.References:

* S/MIME- Week 7: Email Security

* S/MIME &#8211; Wikipedia

* S/MIME Version 3.2 Message Specification

QUESTION 38

Which of the following environmental controls options saves the hardware from humidity and heat, increases hardware performance, and maintains consistent room temperature?
* Hot and cold aisles
* Lighting systern
* Temperature indicator
* EMI shielding
Hot and cold aisles are a type of environmental control that saves the hardware from humidity and heat, increases hardware

performance, and maintains consistent room temperature. Hot and cold aisles are a layout design for data centers, where the server racks are arranged in alternating rows of cold air intake and hot air exhaust. The cold aislefaces the air conditioner output ducts and provides cool air to the front of the servers.

The hot aisle faces the air conditioner return ducts and collects the hot air from the back of the servers. This way, the hot and cold air streams are separated and do not mix, resulting in better cooling efficiency, lower energy consumption, and longer hardware lifespan.References:

* Hot and cold aisles- Week 4: Network Security Controls: Physical Controls

* Hot and Cold Aisles: The Basics of Data Center Cooling

* Hot Aisle vs. Cold Aisle Containment: Which One is Best for Your Data Center?

QUESTION 39

John is working as a network administrator in an MNC company. He was instructed to connect all the remote offices with the corporate office but at the same time deny communication between the remote offices. In this process, he configured a central hub at the corporate head office, through which all branch offices can communicate.

Identify the type of VPN topology implemented by John in the above scenario.
* Star topology
* Hub-and-spoke topology
* Point-to-point topology
* Mesh topology
A hub-and-spoke topology is a type of VPN topology that connects multiple remote offices to a central hub, usually the corporate head office, through VPN tunnels. The hub acts as a gateway for the remote offices to access the corporate network resources. However, the remote offices cannot communicate with each other directly, and have to go through the hub. This topology reduces the number of VPN tunnels required, but also increases the load and latency on the hub. In the scenario, John configured a central hub at the corporate head office, through which all branch offices can communicate, but deniedcommunication between the remote offices.Therefore, the type of VPN topology implemented by John is hub-and-spoke12.References:Network Defense Essentials &#8211; EC-Council Learning,Network Design Scenario #3: Remote Access VPN Design &#8211; Network Defense Blog

QUESTION 40

Messy, a network defender, was hired to secure an organization&#8217;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.
* Signature-based
* Stateful protocol analysis
* Anomaly-based
* Application proxy
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.References:

* Anomaly-Based Intrusion Detection System- Chapter 2: Anomaly-Based Intrusion Detection System

* Network Defense Essentials (NDE) | Coursera- Week 10: Intrusion Detection and Prevention Systems

* A systematic literature review for network intrusion detection system (IDS)- Section 3.2:

Anomaly-based IDS

QUESTION 41

Which of the following techniques protects sensitive data by obscuring specific areas with random characters or codes?
* Data retention
* Data resilience
* Data backup
* Data masking

QUESTION 42

Stephen, a security specialist, was instructed to identify emerging threats on the organization&#8217;s network. In this process, he employed a computer system on the Internet intended to attract and trap those who attempt unauthorized host system utilization to penetrate the organization&#8217;s network.

Identify the type of security solution employed by Stephen in the above scenario.
* Firewall
* Honeypot
* IDS
* Proxy server

QUESTION 43

Daniel, a networking specialist, identifies a glitch in a networking tool and fixes it on a priority using a system.

Daniel was authorized to make a copy of computers programs while maintaining or repairing the system.

Which of the following acts was demonstrated in the above scenario?
* Sarbanes-Oxley Act (SOX)
* The Digital Millennium Copyright Act (DMCA)
* Data Protection Act 2018 (DPA)
* Gramm-Leach-Bliley Act (GLBA)

The DMCA is a US law that aims to protect the rights of digital content creators and owners. It prohibits the unauthorized copying, distribution, modification, or circumvention of digital content, such as software, music, movies, etc. The DMCA also provides exceptions for certain purposes, such as fair use, research, education, or maintenance and repair of systems.In the scenario, Daniel was authorized to make a copy of computer programs while maintaining or repairing the system, which falls under the DMCA exception for system maintenance and repair12.References:Network Defense Essentials &#8211; EC-Council Learning,Network Defense Essentials (NDE) | Coursera

QUESTION 44

Fernandez, a computer user, initiated an action to access a file located on a remote server. In this process, his account went through certain security constraints to check for any restrictions on his account with regard to access to the file.

Which of the following terms is referred to as a file in the above scenario?
* Operation
* Subject
* Reference monitor
* Object

QUESTION 45

Alice purchased a new zip-based document bag and placed white papers related to the academic project.

As it contains confidential information, she locked it with a physical security control that requires a sequence of numbers and letters to unlock.

Identify the type of physical locking system used by Alice in the above scenario.
* Combination lock
* Mechanical lock
* Electromagnetic lock
* Digital lock
A combination lock is a type of physical locking system that requires a sequence of numbers and letters to unlock. The user has to dial or enter the correct combination to open the lock. Combination locks are commonly used for securing luggage, safes, lockers, etc.In the scenario, Alice locked her zip-based document bag with a combination lock that requires a sequence of numbers and letters to unlock12.References:Network Defense Essentials &#8211; EC-Council Learning,Understanding the Various Types of Physical Security Controls

QUESTION 46

Which of the following components of VPN is used to manage tunnels and encapsulate private data?
* Remote network
* VPN protocol
* Network access server
* VPN client
A VPN protocol is a component of VPN that is used to manage tunnels and encapsulate private data. A VPN protocol defines the rules and standards for establishing and maintaining a secure connection between the VPN client and the VPN server. A VPN protocol also specifies how the data is encrypted, authenticated, and transmitted over the tunnel.Some common VPN protocols are IPSec, SSL/TLS, PPTP, L2TP, and OpenVPN12.References:Network Defense Essentials &#8211; EC-Council Learning,VPN Protocols Explained & Compared: OpenVPN, IPSec, PPTP, IKEv2

QUESTION 47

Peter, a network defender, was instructed to protect the corporate network from unauthorized access. To achieve this, he employed a security solution for wireless communication that uses dragonfly key exchange for authentication, which is the strongest encryption algorithm that protects the network from dictionary and key recovery attacks.

Identify the wireless encryption technology implemented in the security solution selected by Peter in the above scenario.
* WPA
* WPA3
* EAP
* WEP

WPA3 is the latest standard of Wi-Fi Protected Access, which was released in 2018 by the Wi-Fi Alliance.

WPA3 uses a new handshake protocol called Simultaneous Authentication of Equals (SAE), which is based on a zero-knowledge proof known as dragonfly. Dragonfly is a key exchange algorithm that uses discrete logarithm cryptography to derive a shared secret between two parties, without revealing any information about their passwords or keys. Dragonfly is resistant to offline dictionary attacks, where an attacker tries to guess the password by capturing the handshake and testing different combinations. Dragonfly is also resistant to key recovery attacks, where an attacker tries to recover the encryption key by exploiting weaknesses in the algorithm or implementation. Dragonfly provides forward secrecy, which means that even if an attacker manages to compromise the password or key in the future, they cannot decrypt the past communication.

WPA3 also supports other features such as increased key sizes, opportunistic wireless encryption, and protected management frames, which enhance the security and privacy of wireless networks.References:

* WPA3 Dragonfly Handshake

* WPA3 Encryption and Configuration Guide

* Dragon Fly &#8211; Zero Knowledge Proof

* What is SAE (Simultaneous Authentication of Equals)?

* Dragonfly &#8211; people.scs.carleton.ca

QUESTION 48

An loT sensor in an organization generated an emergency alarm indicating a security breach. The servers hosted in an loT layer accepted, stored, and processed the sensor data received from loT gateways and created dashboards for monitoring, analyzing, and implementing proactive decisions to tackle the issue.

Which of the following layers in the loT architecture performed the above activities after receiving an alert from the loT sensor?
* Device layer
* Cloud layer
* Process layer
* Communication Layer
The cloud layer of IoT architecture is the layer that hosts the servers that accept, store, and process the sensor data received from IoT gateways. The cloud layer also creates dashboards for monitoring, analyzing, and implementing proactive decisions to tackle the issue. The cloud layer provides scalability, reliability, and security for the IoT system.The cloud layer can use various cloud computing models, such as public, private, hybrid, or community clouds12.References:Network Defense Essentials &#8211; EC-Council Learning,IoT Architecture: The 4 Layers of an IoT System

QUESTION 49

Stella, a mobile user, often ignores the messages received from the manufacturer for updates. One day, she found that files in her device are being replaced, she immediately rushed to the nearest service center for inquiry. They tested the device and identified vulnerabilities in it as it ran with an obsolete OS version.

Identify the mobile device security risk raised on Stella&#8217;s device in the above scenario.
* Application-based risk
* System-based risk
* Network-based risk

* Physical security risks
System-based risk is a type of mobile device security risk that arises from the vulnerabilities or flaws in the operating system or firmware of the device. System-based risk can expose the device to malware, spyware, ransomware, or other malicious attacks that can compromise the data, functionality, or privacy of the device.

System-based risk can be mitigated by applying regular security updates and patches from the manufacturer or vendor, as well as using antivirus or anti-malware software. In the above scenario, Stella&#8217;s device faced a system-based risk, as it ran with an obsolete OS version that had vulnerabilities that allowed the files to be replaced. She ignored the messages from the manufacturer for updates, which could have prevented the risk.

References:

* Mobile Device Security Risks- Week 8: Mobile Device Security

* Is It Safe to Use an Old or Used Phone? Here&#8217;s What You Should Know

* Obsolete products &#8211; The National Cyber Security Centre

QUESTION 50

Kalley, a network administrator of an organization, has installed a traffic monitoring system to capture and report suspicious traffic signatures. In this process, she detects traffic containing password cracking, sniffing, and brute-forcing attempts.Which of the following categories of suspicious traffic signature were identified by Kalley through the installed monitoring system?
* Reconnaissance signatures
* Unauthorized access signatures
* Denial-of-service (DoS) signatures
* Informational signatures
Unauthorized access signatures were identified by Kalley through the installed monitoring system.

Unauthorized access signatures are designed to detect attempts to gain unauthorized access to a system or network by exploiting vulnerabilities, misconfigurations, or weak credentials. Password cracking, sniffing, and brute-forcing are common techniques used by attackers to obtain or guess the passwords of legitimate users or administrators and gain access to their accounts or privileges. These techniques generate suspicious traffic patterns that can be detected by traffic monitoring systems, such as Snort, using signature-based detection.

Signature-based detection is based on the premise that abnormal or malicious network traffic fits a distinct pattern, whereas normal or benign traffic does not. Therefore, by installing a traffic monitoring system and capturing and reporting suspicious traffic signatures, Kalley can identify and prevent unauthorized access attempts and protect the security of her organization&#8217;s network.References:

* Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-33 to 3-34

* Detecting Suspicious Traffic via Signatures &#8211; Intrusion Detection with Snort, O&#8217;Reilly, 2003

* Threat Signature Categories &#8211; Palo Alto Networks, Palo Alto Networks, 2020

QUESTION 51

Peter, a security professional, was hired by an organization and was instructed to secure the application and its content from unauthorized access. In this process, Peter implemented a public-key cryptosystem that uses modular arithmetic and elementary number theory for Internet encryption and user authentication.

Which of the following algorithms was employed by Peter in the above scenario?
* RSA
* MD6
* DSA
* SHA-2

RSA is a public-key cryptosystem that uses modular arithmetic and elementary number theory for Internet encryption and user authentication. RSA stands for Rivest-Shamir-Adleman, the names of the inventors of the algorithm. RSA allows users to generate a pair of keys, one public and one private, that are mathematically related. The public key can be used to encrypt messages or verify digital signatures, while the private key can be used to decrypt messages or create digital signatures.RSA is based on the difficulty of factoring large numbers, which makes it secure and widely used12.References:What is Public-Key Cryptosystem in Information Security?,Network Defense Essentials (NDE) | Coursera

QUESTION 52

Joseph, a security professional, was instructed to secure the organization&#8217;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.
* Composite-signature-based analysis
* Context-based signature analysis
* Content-based signature analysis
* Atomic-signature-based analysis

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.References:

* [Understanding the Network Traffic Signatures] &#8211; Module 12: Network Traffic Monitoring

* Network Defense Essentials (NDE) | Coursera- Week 12: Network Traffic Monitoring

* [Network Defense Essentials Module 12 (Network Traffic Monitoring) &#8211; Quizlet] &#8211; Flashcards: What are Network Traffic Signatures?

QUESTION 53

Mark, a network administrator in an organization, was assigned the task of preventing data from falling into the wrong hands. In this process, Mark implemented authentication techniques and performed full memory encryption for the data stored on RAM.

In which of the following states has Steve encrypted the data in the above scenario?
* Data in use
* Data in transit
* Data inactive
* Data in rest

The state in which Mark encrypted the data in the above scenario is data in use. Data in use refers to data that is being processed or manipulated by an application or a system, such as data stored on RAM or CPU registers. Data in use is the most vulnerable state of data, as it is exposed to various threats, such as memory scraping, buffer overflow, or side-channel attacks, that can compromise the confidentiality, integrity, or availability of the data. Data in use encryption is a technique that protects the data while it is being processed by encrypting it in memory using hardware or software solutions. Data in use encryption prevents unauthorized access or modification of the data, even if the system is compromised or the memory is dumped.Data in use encryption is one of the three types of data encryption, along with data at rest encryption and data in transit encryption123.References:

* Network Defense Essentials Courseware, EC-Council, 2020, pp. 3-23 to 3-24

* Encryption: Data at Rest, Data in Motion and Data in Use, Jatheon, 2020

* Data in Use Encryption: What It Is and Why You Need It, Fortanix, 2020