212-82 Q&As

Certified Cybersecurity Technician(C|CT)

Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/212-82.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Camden, a network specialist in an organization, monitored the behavior of the organizational network using SIFM from a control room. The SIEM detected suspicious activity and sent an alert to the camera. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers.

Which of the following SIEM functions allowed Camden to view suspicious behavior and make correct decisions during a security incident?

A. Application log monitoring

B. Log Retention

C. Dashboard

D. Data aggregation

Correct Answer: C

Explanation: Dashboard is the SIEM function that allowed Camden to view suspicious behavior and make correct decisions during a security incident. SIEM (Security Information and Event Management) is a system or software that collects, analyzes, and correlates security data from various sources, such as logs, alerts, events, etc., and provides a centralized view and management of the security posture of a network or system. SIEM can be used to detect, prevent, or respond to security incidents or threats. SIEM consists of various functions or components that perform different tasks or roles. Dashboard is a SIEM function that provides a graphical user interface (GUI) that displays various security metrics, indicators, alerts, reports, etc., in an organized and interactive manner. Dashboard can be used to view suspicious behavior and make correct decisions during a security incident. In the scenario, Camden monitored the behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to Camden. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers. This means that he used the dashboard function of SIEM for this purpose. Application log monitoring is a SIEM function that collects and analyzes application logs, which are records of events or activities that occur within an application or software. Log retention is an SIEM function that stores and preserves logs for a certain period of time or indefinitely for future reference or analysis. Data aggregation is an SIEM function that combines and normalizes data from different sources into a common format or structure.

QUESTION 2

Anderson, a security engineer, was Instructed to monitor all incoming and outgoing traffic on the organization\\'s network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.

Identify the type of attack signature analysis performed by Anderson in the above scenario.

A. Context-based signature analysis

B. Atomic-signature-based analysis

C. Composite-signature-based analysis

D. Content-based signature analysis

Correct Answer: D

Explanation: Content-based signature analysis is the type of attack signature analysis performed by Anderson in the above scenario. Content-based signature analysis is a technique that analyzes packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit. Content-based signature analysis can help detect attacks that manipulate packet headers to evade detection or exploit vulnerabilities . Context-based signature analysis is a technique that analyzes packet payloads such as application data or commands to check whether they match any known attack patterns or signatures. Atomic-signature-based analysis is a technique that analyzes individual packets to check whether they match any known attack patterns or signatures. Composite-signature-based analysis is a technique that analyzes multiple packets or sessions to check whether they match any known attack patterns or signatures.

QUESTION 3

An attacker with malicious intent used SYN flooding technique to disrupt the network and gain advantage over the network to bypass the Firewall. You are working with a security architect to design security standards and plan for your organization. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Study the Synflood.pcapng file and determine the source IP address.

Note: Synflood.pcapng file is present in the Documents folder of Attacker-1 machine.

A. 20.20.10.180

B. 20.20.10.19

C. 20.20.10.60

D. 20.20.10.59

Correct Answer: B

Explanation: 20.20.10.19 is the source IP address of the SYN flooding attack in the above scenario. SYN flooding is a type of denial-of-service (DoS) attack that exploits the TCP (Transmission Control Protocol) three-way handshake process

to disrupt the network and gain advantage over the network to bypass the firewall. SYN flooding sends a large number of SYN packets with spoofed source IP addresses to a target server, causing it to allocate resources and wait for the

corresponding ACK packets that never arrive. This exhausts the server\\'s resources and prevents it from accepting legitimate requests . To determine the source IP address of the SYN flooding attack, one has to follow these steps:

Navigate to the Documents folder of Attacker-1 machine. Double-click on Synflood.pcapng file to open it with Wireshark. Click on Statistics menu and select Conversations option. Click on TCP tab and sort the list by Bytes column in

descending order. Observe the IP address that has sent the most bytes to 20.20.10.26 (target server).

The IP address that has sent the most bytes to 20.20.10.26 is 20.20.10.19 , which is the source IP address of the SYN flooding attack.

QUESTION 4

A software company has implemented a wireless technology to track the employees\\' attendance by recording their in and out timings. Each employee in the company will have an entry card that is embedded with a tag. Whenever an

employee enters the office premises, he/she is required to swipe the card at the entrance. The wireless technology uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects.

Which of the following technologies has the software company implemented in the above scenario?

A. WiMAX

B. RFID

C. Bluetooth

D. Wi-Fi

Correct Answer: B

Explanation: RFID (Radio Frequency Identification) is the wireless technology that the software company has implemented in the above scenario. RFID uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects1112. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless technology that provides high-speed broadband access over long distances13. Bluetooth is a wireless technology that enables short-range data communication between devices, such as phones, laptops, printers, etc.14. Wi-Fi (Wireless Fidelity) is a wireless technology that allows devices to connect to a local area network or the internet using radio waves

QUESTION 5

A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with http://securityabc.s21sec.com.

A. 5.9.200.200

B. 5.9.200.150

C. 5.9.110.120

D. 5.9.188.148

Correct Answer: D

Explanation: 5.9.188.148 is the IP address linked with http://securityabc.s21sec.com in the above scenario. A threat intelligence feed is a source of data that provides information about current or potential threats and attacks that can affect an

organization\\'s network or system. A threat intelligence feed can include indicators of compromise (IoCs), such as IP addresses, domain names, URLs, hashes, etc., that can be used to detect or prevent malicious activities. To analyze the

threat intelligence feed data file and determine the IP address linked with http://securityabc.s21sec.com, one has to follow these steps:

Navigate to the Documents folder of Attacker-1 machine.

Open Threatfeed.txt file with a text editor.

Search for http://securityabc.s21sec.com in the file.

Observe the IP address associated with the URL.

The IP address associated with the URL is 5.9.188.148, which is the IP address linked with http://securityabc.s21sec.com.

QUESTION 6

Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.

Which of the following rules of evidence was discussed in the above scenario?

A. Authentic

B. Understandable

C. Reliable

D. Admissible

Correct Answer: D

Explanation: Admissible is the rule of evidence discussed in the above scenario. A rule of evidence is a criterion or principle that determines whether a piece of evidence can be used in a legal proceeding or investigation. Admissible is a rule of evidence that states that the evidence must be relevant, reliable, authentic, and understandable to be accepted by a court or a jury . Admissible also means that the evidence must be obtained legally and ethically, without violating any laws or rights. In the scenario, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury, which means that he has followed the admissible rule of evidence. Authentic is a rule of evidence that states that the evidence must be original or verifiable as genuine and not altered or tampered with. Understandable is a rule of evidence that states that the evidence must be clear and comprehensible to the court or jury and not ambiguous or confusing. Reliable is a rule of evidence that states that the evidence must be consistent and trustworthy and not based on hearsay or speculation.

QUESTION 7

The incident handling and response (IHandR) team of an organization was handling a recent cyberattack on the organization\\'s web server. Fernando, a member of the IHandP team, was tasked with eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. For this purpose. Fernando applied the latest patches to the web server and installed the latest security mechanisms on it. Identify the IHandR step performed by Fernando in this scenario.

A. Notification

B. Containment

C. Recovery

D. Eradication

Correct Answer: D

Explanation: Eradication is the IHandR step performed by Fernando in this scenario. Eradication is a step in IHandR that involves eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future.

Eradication can include applying patches, installing security mechanisms, removing malware, restoring backups, or reformatting systems.

References: [Eradication Step in IHandR]

QUESTION 8

An organization hired a network operations center (NOC) team to protect its IT infrastructure from external attacks. The organization utilized a type of threat intelligence to protect its resources from evolving threats. The threat intelligence helped the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors.

Identify the type of threat intelligence consumed by the organization in the above scenario.

A. Operational threat intelligence

B. Strategic threat intelligence

C. Technical threat intelligence

D. Tactical threat intelligence

Correct Answer: C

Explanation: Technical threat intelligence is a type of threat intelligence that provides information about the technical details of specific attacks, such as indicators of compromise (IOCs), malware signatures, attack vectors, and vulnerabilities. Technical threat intelligence helps the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors. Technical threat intelligence is often consumed by security analysts, incident responders, and penetration testers who need to analyze and respond to active or potential threats.

QUESTION 9

Dany, a member of a forensic team, was actively involved in an online crime investigation process. Dany\\'s main responsibilities included providing legal advice on conducting the investigation and addressing legal issues involved in the forensic investigation process. Identify the role played by Dany in the above scenario.

A. Attorney

B. Incident analyzer

C. Expert witness

D. Incident responder

Correct Answer: A

Explanation: Attorney is the role played by Dany in the above scenario. Attorney is a member of a forensic team who provides legal advice on conducting the investigation and addresses legal issues involved in the forensic investigation

process. Attorney can help with obtaining search warrants, preserving evidence, complying with laws and regulations, and presenting cases in court3. References: Attorney Role in Forensic Investigation

QUESTION 10

An IoT device placed in a hospital for safety measures has sent an alert to the server. The network traffic has been captured and stored in the Documents folder of the "Attacker Machine-1". Analyze the IoTdeviceTraffic.pcapng file and identify the command the IoT device sent over the network.

A. Tempe_Low

B. Low_Tem p e

C. High_Tcmpe

D. Temp_High

Correct Answer: D

Explanation: The IoT device sent the command Temp_High over the network, which indicates that the temperature in the hospital was above the threshold level. This can be verified by analyzing the IoTdeviceTraffic.pcapng file using a network protocol analyzer tool such as Wireshark4. The command Temp_High can be seen in the data field of the UDP packet sent from the IoT device (192.168.0.10) to the server (192.168.0.1) at 12:00:03. The screenshot below shows the packet details5: References: Wireshark User\\'s Guide, [IoTdeviceTraffic.pcapng]

QUESTION 11

Jordan, a network administrator in an organization, was instructed to identify network- related issues and improve network performance. While troubleshooting the network, he received a message indicating that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host, which of the following network issues did Jordan find in this scenario?

A. Time exceeded message

B. Destination unreachable message

C. Unreachable networks

D. Network cable is unplugged

Correct Answer: B

Explanation: Destination unreachable message is the network issue that Jordan found in this scenario. Destination unreachable message is a type of ICMP message that indicates that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host. Destination unreachable message can be caused by various reasons, such as incorrect routing, firewall blocking, or host configuration problems1. References: Destination Unreachable Message

QUESTION 12

Ayden works from home on his company\\'s laptop. During working hours, he received an antivirus software update

notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel. Which of the following PCI-DSS requirements is demonstrated In this scenario?

A. PCI-DSS requirement no 53

B. PCI-DSS requirement no 1.3.1

C. PCI-DSS requirement no 5.1

D. PCI-DSS requirement no 1.3.2

Correct Answer: A

Explanation: PCI-DSS requirement no 5.3 is the PCI-DSS requirement that is demonstrated in this scenario. PCI-DSS (Payment Card Industry Data Security Standard) is a set of standards that applies to entities that store, process, or transmit payment card information, such as merchants, service providers, or payment processors. PCI-DSS requires them to protect cardholder data from unauthorized access, use, or disclosure. PCI-DSS consists of 12 requirements that are grouped into six categories: build and maintain a secure network and systems, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy. PCI-DSS requirement no 5.3 is part of the category "maintain a vulnerability management program" and states that antivirus mechanisms must be actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. In the scenario, Ayden works from home on his company\\'s laptop. During working hours, he received an antivirus software update notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel. This means that his company\\'s laptop has an antivirus mechanism that is actively running and cannot be disabled or altered by users, which demonstrates PCI-DSS requirement no 5.3.

QUESTION 13

Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit.

Which of the following keys did Louis use to verify the digital signature in the above scenario?

A. Riley\\'s public key

B. Louis\\'s public key

C. Riley\\'s private key

D. Louis\\'s private key

Correct Answer: A

Explanation: Riley\\'s public key is the key that Louis used to verify the digital signature in the above scenario. A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. A digital signature is created by applying a hash function to the message or document and then encrypting the hash value with the sender\\'s private key. A digital signature can be verified by decrypting the hash value with the sender\\'s public key and comparing it with the hash value of the original message or document . Riley\\'s public key is the key that corresponds to Riley\\'s private key, which he used to sign the message. Louis\\'s public key is the key that corresponds to Louis\\'s private key, which he may use to encrypt or decrypt messages with Riley. Louis\\'s private key is the key that only Louis knows and can use to sign or decrypt messages. Riley\\'s private key is the key that only Riley knows and

can use to sign or encrypt messages.

QUESTION 14

Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64

B. 128

C. 255

D. 138

Correct Answer: B

Explanation: 128 is the TTL value that Henry obtained, which indicates that the target OS is Windows. TTL (Time to Live) is a field in the IP (Internet Protocol) header that specifies how long a packet can remain in a network before it is discarded or dropped. TTL is usually expressed in seconds or hops (the number of routers or gateways that a packet passes through). TTL is used to prevent packets from looping endlessly in a network or consuming network resources . Different operating systems have different default TTL values for their packets. By observing the TTL value of a packet from a target system or network, one can infer the operating system of the target . Some common TTL values and their corresponding operating systems are:

64: Linux, Unix, Android

128: Windows

255: Cisco IOS

60: Mac OS

In the scenario, Henry used Nmap tool to discover the OS of the target system. Nmap (Network Mapper) is a tool that can perform various network scanning and enumeration tasks, such as port scanning, OS detection, service identification,

etc . Nmap can use various techniques to detect the OS of a target system, such as TCP/IP fingerprinting, which involves analyzing various TCP/IP characteristics of packets from the target system, such as TTL value. In the scenario, Henry

obtained a TTL value of 128 , which indicates that the target OS is Windows.

QUESTION 15

Giovanni, a system administrator, was tasked with configuring permissions for employees working on a new project. Hit organization used active directories (ADs) to grant/deny permissions to resources Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. Identify the type of account created by Giovanni in this scenario.

A. Third-party account

B. Croup-based account

C. Shared account

D. Application account

Correct Answer: B

Explanation: Group-based account is the type of account created by Giovanni in this scenario. An account is a set of credentials, such as a username and a password, that allows a user to access a system or network. An account can have different types based on its purpose or usage. A group-based account is a type of account that allows multiple users to access a system or network with the same credentials and permissions. A group-based account can be used to simplify the management of users and resources by assigning them to groups based on their roles or functions. In the scenario, Giovanni was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. This means that he created a group-based account for those employees. A third-party account is a type of account that allows an external entity or service to access a system or network with limited permissions or scope. A shared account is a type of account that allows multiple users to access a system or network with the same credentials but different permissions. An application account is a type of account that allows an application or software to access a system or network with specific permissions or functions.